Department Policy No. DIR-005a-13

Title:	"Scanning & Tossing" of Public Records
Authorizing Source:	Ch. 40.14 RCW Ch. 434-662 WAC; Ch. 434-663 WAC; WA State Archives: "Requirements for the Destruction of Non-Archival Paper Records after Imaging"
References:	State General Records Retention Schedule; Military Department Records Retention Schedule; Public Schools (K-12) Records Retention Schedule; WMD Form 0007-13; WMD Form 0008-13
Information Contact:	Washington Military Department Records Officer Building 1 (253) 512-8108
Effective Date:	September 11, 2013
Mandatory Review Date:	September 23, 2026
Revised:	September 23, 2022
Approved By:	Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

Purpose

Provide the requirements and guidelines to lawfully destroy eligible paper-based source records after they have been converted to a digital format by imaging (also known as "scanning & tossing").

Scope

This policy applies to all Washington Military Department (WMD) paper-based source records that are created, received, or maintained by the WMD in connection with the transaction of public business. Any WMD employee or volunteer who creates, receives, or maintains WMD public records must comply with this policy.

Policy

The WMD generally encourages conversion of paper-based source records to electronic formats, also known as "scanning and tossing," when practical and authorized in accordance with the requirements of this policy.

A. Requirements for Scanning and Tossing

WMD employees can implement the scanning and tossing of paper-based source records as long as the following requirements are met:

1. The records MUST be "NON-ARCHIVAL" and covered by a current, approved records retention schedule by the State Records Committee in accordance with RCW 40.14.050.
2. The records MUST be scanned and verified in a systematic and consistent fashion that ensures a complete and accurate copy of the source record in accordance with the guidelines in the "Destruction Authorization for Records after Imaging" form. Paper-based source records that have not been imaged completely and accurately must not be destroyed.
3. Images MUST be accessible and protected for the entire required retention period.
4. The records are **not** required for or subject to any of the following:
    a) Existing public records requests in accordance with chapter 42.56 RCW; or
    b) Ongoing or reasonable anticipated litigation; or
    c) Other legal requirements, federal statues, grant agreements, audits, etc. that specifically requires retention of the original paper-based source record; or
    d) Archival transfer.

Procedures

1. Records Coordinators and/or Records Custodians, in coordination with work unit staff, will:
    a) Determine which records series and specific types of records the work unit would like to scan and toss.
    b) Document the proposed scanning and tossing procedure on a Scanning and Tossing Quality Assurance Procedure Template (WMD Form 0008-13).
    c) Complete sections 1-4 of the Scanning and Tossing Approval Form (WMD Form 0007-13).
        i) For section 1, see definitions for "record series," "disposition authority number," and "categories of information" in this policy.
    d) Submit the template and form to the WMD Records Officer.

2. The WMD Records Officer will verify storage capacity requirements of the network location for the requested records with the Information Technology (IT) Division:
    a) The WMD Records Officer will submit the Scanning and Tossing Approval Form to the IT helpdesk.
    b) IT will review the proposed file server location, capacity needs, and security needs identified in section 1 of the form.
    c) IT will assess server storage and security capabilities, including whether or not the proposed file server location can accommodate the initial and ongoing capacity and level of security needed for the imaged records.
        i) If IT finds that the proposed file server location cannot accommodate the capacity and security indicated on the form, IT will:
            (1) Identify an alternate file server location and indicate the path of the location on the form.
            (2) Set up a folder in the alternate location and grant appropriate permissions to work unit staff. (Contact the WMD Records Officer to determine which staff will need to access the folder.)
        ii) If IT cannot find a suitable file server location and/or cannot approve storage of the imaged records on the state network, IT will notify the WMD Records Officer and provide an explanation. In that case, the WMD Records Officer will work with the Records Coordinator/Custodian who submitted the form to determine whether IT's concerns may be addressed, and if necessary, submit a new procedure template and approval form for IT review.
    d) The IT will:
        i) Sign section 5 of the form to authorize storage of the imaged records on the state network.
        ii) Return the form to the WMD Records Officer by campus mail.
        iii) Close the helpdesk ticket.
3. The WMD Records Officer will:
    a) Sign section 6 of the form and date the top of the form to authorize destruction of imaged records.
    b) Provide a copy of the signed form to the Records Coordinator/Custodian and IT.
    c) File the original signed form and copy of the procedure template.
4. The Records Coordinator/Custodian will provide the WMD Records Officer an updated inventory spreadsheet for the record series approved for scanning and tossing, if necessary.

Definitions

Archival Records: Records that are subject to permanent retention at the Washington State Archives. To determine whether a record is archival or non-archival, see the "Designation" column on the right side of the retention schedule.

Categories of Information:

Category 1 – Public Information: Information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

Category 2 – Sensitive Information: May not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information: Information that is specifically protected from disclosure by law. It may include but is not limited to:

- Personal information as defined in RCW 42.56.590 and RCW 19.255.010.
- Information about public employees as defined in RCW 42.56.250.
- Lists of individuals for commercial purposes as defined in RCW 42.56.070 (9).
- Information regarding IT infrastructure and security of computer and telecommunications networks as defined in RCW 42.56.420.

Other examples include, but are not limited to:

- FERPA Information – Student records, grades, class enrollment, etc.
- Payment Card Industry Information – Credit card numbers, PINS, verification codes, etc.

Category 4 – Confidential Information Requiring Special Handling: Information that is specifically protected from disclosure by law and for which:

- Especially strict handling requirements are dictated, such as by statute, regulation, or agreement.
- Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Disposition Authority Number (DAN): Control numbers systematically assigned to records series or records retention schedules when they are approved by the State Records Committee.

Imaging: Converting paper documents into digital documents. Approval is required to destroy the paper documents per Chapter 434-663 WAC.

Non-Archival Records: Records that are not subject to permanent retention at the Washington State Archives. To determine whether a record is archival or non-archival, see the "Designation" column on the right side of the retention schedule.

Record Series: A group of records performing a specific function that is used and filed together and may be transferred or destroyed together. Records series are defined in the

State General Records Retention Schedule and WMD Unique Records Retention Schedule.

Scanning and Tossing: The process of destroying paper-based source records after conversion into a digital format through imaging.

Work Unit: A WMD division, unit, section, or office. For the purposes of records management, work units are typically WMD divisions.