Electronic Document Management System

Policies and Minimum Functional and Procedural Standards for an EDMS

Requirement Area	Detail
General Functional Standards	• Ability to capture, manage, and retrieve records • Ability to implement and maintain metadata tagging • Ability to maintain record integrity • Ability to provide open standards interfaces, including accepting and filing records from producing applications and the routing of documents • Ability to support applicable security standards and activity audit tracking • Ability to handle document disposal
Document Retention and Disposal Policies	• Electronic documents must be maintained for their full retention periods • Electronic case documents with long-term retention requirements must be migrated to new file formats before technology becomes obsolete • Electronic case documents must remain accessible as hardware and software technology changes; IT staff must migrate electronic documents whenever new technology is upgraded or changed • Electronic case documents that are not transferred to Archives of Michigan must be disposed by overwriting or degaussing • Backup capability must exist and must ensure synchronization between all record category, file plan, folder, record metadata, and content repositories

Authenticity of Electronic Case Documents and Data:
An electronic case record (both data and documents) is useful only if it continues to exist in a form that allows it to be retrieved, and, after retrieved, provides reliable and authentic evidence of the activity that produced the record. This is referred to as digital continuity or record integrity.

The authenticity of an electronic record can be demonstrated by verifying that:

- the right document and/or data was put into storage properly;
- either nothing happened in storage to change this document and/or data or, alternatively, any changes in the document and/or data over time are insignificant;
- all the correct documents and/or data and only the correct documents and/or data were retrieved from storage;
- the processing was executed correctly to output an authentic reproduction of the record;
- appropriate security technology and procedures are in place and followed by all;
- activity audit tracking is in place for both the system and documents.

Authenticity can also be demonstrated by verifying that security and auditing are in place and that the files and metadata are consistent with what was originally stored by the EDMS. To save metadata about electronically born records and to maintain as much functionality as

possible, we recommend that electronically born records be retained in their native format until it is necessary to migrate the records (see Maintenance of Electronic Case Data and Documents for Retention Period below for details).

EDMS Requirements:

- Courts are required to store electronic case documents in an EDMS to ensure the ability to use information in the way needed, for its retention requirements. This requires active management of information through change so that it remains complete, available, and usable in the way needed.
- As electronic filing is implemented, courts can choose the MiFILE Cloud DMS or purchase their own systems. Digital imaging systems that are used to produce electronic images of paper documents through use of scanning equipment are not necessarily electronic document management systems.
- Courts must not store electronic case documents on an office drive; the EDMS will typically have its own server(s) with the features described in this document, including security and activity audit tracking.
- A court that purchases its own EDMS or that uses a digital imaging system to store electronic case documents must comply with these standards, must back up the EMDS regularly, and must have a disaster recovery plan in place.

1. EDMS Functional Standards (Required):
    a. General Requirements
        1) Ability to capture, manage, and retrieve records
        2) Ability to implement and maintain metadata tagging
        3) Ability to maintain record integrity
        4) Ability to provide open standards interfaces, including accepting and filing records from producing applications and support to workflow
        5) Ability to support applicable security standards and activity audit tracking
        6) Ability to handle document disposal
    b. Specific Requirements
        1) Capturing, Managing, and Retrieving Records
            a) Ability to create, edit, and delete file plan components and identifiers
            Mandatory File Plan Components
                - Record category name
                - Record category identifier
                - Record category description
                - Disposition instructions
                - Disposition authority
                - Transfer to Archives indicator
            b) Ability to create, edit, and delete record folder components and identifiers
            c) Ability to create, edit, and delete metadata elements or attributes

Mandatory Record Metadata Components

- Record identifiers, marking, and indicators
- Record descriptors (media type and format)
- Record dates
- Producing application and version, and PDF version

d) Ability to capture and populate metadata
e) Ability to capture and store transmission and receipt data from e-Filing system
f) Ability to capture (scan) documents
g) Ability to file, annotate, and redact
h) Ability to search, view, copy, save, store, and print
i) Ability to schedule records for retention and disposal
j) Ability to associate attributes of a record folder to a record
k) Ability to support all SCAO-prescribed electronic formats
l) Ability to store e-mails
m) Repository (direct access device on which electronic records and metadata are stored)
n) Storage space for nonactive records
o) Storage availability and monitoring (including offsite storage)

2) Maintaining Integrity
   a) Ability to control access
      - define, update, assign permissions
      - view, modify, copy, link, print records and metadata
      - prevent unauthorized access to repository
      - export, backup, and remove audit files
   b) Addition, designation, and version control, including ability to revert to previous document versions
   c) Audit functions
      - Ability to log actions, date, time, object identifiers, and user identifiers for user accounts, user groups, records and record folders, associated metadata elements, and file plan components
      - Audit analysis functionality
   d) Ability to read and process stored records in same manner as original by using any of the following methods
      - backward compatibility
      - maintaining hardware and software used to create or capture the record
      - maintaining hardware and software capable of viewing the record in its native format
      - migrating the record to a new format before the old format becomes obsolete
   e) Safeguard/lockout/timeout features
   f) Ability to backup stored records

g) Ability to store backup copies off-line and at separate location(s) to safeguard against loss
h) Data integrity and disaster recovery capability
i) Rebuild capability; necessary for reconstructing records management environment after a disaster.

3) Records Disposal (includes transfer and destruction)
a) Ability to schedule records for retention and disposal (records management feature)
b) Ability to secure access, maintain context within a record series, and execute disposition instructions for all records in the system (records management feature)
c) Ability to preserve a record's required metadata (records management feature)
d) Ability to transfer required electronic documents and any associated metadata to the Archives of Michigan at the end of the relevant retention periods prescribed in the retention schedule. Court must contact Archives for guidance.

2. Maintenance of Electronic Case Data and Documents for Retention Period:
a. Courts are required to maintain electronic case data and documents for their full retention periods as prescribed in the retention schedule.
b. Most electronic case data and documents will be kept longer than the original technology that was used to create them and new technology is not always compatible with older technology. Long-term retention of electronic records must be achieved in a manner that protects the records from degradation, loss of content, or inability to access. Therefore, in order to ensure electronic case documents can be used in the way needed for as long as needed, the documents should not be stored in their original software format and on their original storage media for their entire retention period.
c. Courts must ensure that all electronic case documents with long-term retention requirements are migrated to a new file format before the technology becomes obsolete. Long-term retention means the life of an electronic record is expected to be longer than the life of the technology used. This is generally about 10 years, but it can vary.
d. Courts are also responsible for ensuring that all electronic records remain accessible as technology is upgraded or changed. Each time technology upgrades, courts should inform their information technology staff of the need to migrate their electronic case data and documents to the new technology.
e. Backup capability must ensure synchronization between all record category, file plan, folder, record metadata, and content repositories. Backup copies must be destroyed in accordance with the retention schedule. Backup processes should be tested to ensure they are copying all of the records and data as intended.

EDMS Recommended Features:

- Document imaging and workflow integration to support the creation and management of electronic documents and related data, and to maximize productivity.
- Retrieval assistance and free-text search (not just search capability of metadata).
- Ability to make global changes to record category names, record category identifiers, and disposition components.
- Ability to reorganize file plan and automatically propagate the changes from the reorganization.
- Ability to bulk load a file plan, electronic records, and record metadata.
- Interfaces with case management system, e-mail, word processing, MiFILE, and other applications.
- Ability to write and generate reports.
- Web capability and viewer.

EDMS Policies:

Any provider of a system that creates, receives, maintains, uses, and disposes of court records, whether at the state or the local level, is prohibited from selling, transferring, or otherwise using those court records, except as authorized by law, Michigan court rule, or the Michigan Supreme Court.

Any Michigan court that enters into a contract with a system provider for an electronic filing system, a case management system, or a document management system that creates, receives, maintains, uses, and disposes of court records shall ensure that the following provisions are included in the contract:

- The provider shall not sell, transfer, or otherwise use a court record, except as authorized by state law, court rule, or the Michigan Supreme Court.
- The provider shall dispose of records in compliance with statutes, court rules, and the standards established by the SCAO.
- If the contract with the provider is terminated, the provider shall ensure that all records are returned to the court or authorized custodian of those records. Duplicate records shall be destroyed in accordance with the standards established by the SCAO and the provider shall execute a signed certificate of media disposition stating that the data has been destroyed in accordance with those standards.

Any Michigan court that shares an electronic filing system, a case management system, or a document management system with the executive branch shall sign a memorandum of understanding, approved by the Michigan Supreme Court, regarding the creation, receipt, maintenance, use, and disposal of court records in that system. An individual court does not need to have a memorandum of understanding if the Michigan Supreme Court has a statewide memorandum of understanding with the executive branch agency that shares the system.

Whenever a court converts from one electronic filing system, case management system, or document management system to another, it must establish policies and procedures that ensure that all records are accessible in their entirety for the retention period of the related records, as prescribed in the retention schedule.

Any person who retains possession of and refuses to deliver any records of the courts of Michigan upon demand by the authorized custodian of those records shall be guilty of a misdemeanor, punishable by imprisonment in the state prison not more than 2 years or by a fine of not more than $1,000. MCL 750.491.

An electronic case management system and document management system must be capable of transferring required data, electronic documents, and any associated metadata to the Archives of Michigan at the end of the relevant retention periods prescribed in the retention schedule and in the manner prescribed by Archives and the SCAO.

Source: Michigan Trial Court Records Management Standards, Standard 3.1.2.3. Electronic Case Data and Documents. Established by the State Court Administrative Office, February 14, 2019.