Manual Notice  2014-1

From: Dana Glover, Director, Research and Technology Implementation Office


Effective Date: December 19, 2014

Purpose

The purpose of this manual notice is to issue changes to Chapters 1, 2, 4, 5, 7 and 10 of the Records Management Manual.

Changes

Throughout manual: Revise all references to General Services Division (GSD) to Research and Technology Office (RTI).

Remove references to Regions (DDOR to DDO).

Chapter 1, Program Overview:

◆ Section 1, minor text revisions.

◆ Section 2, subsection Program Responsibilities
  ● The Records Management Program is responsible for….  
    ● Add bullet: oversight and monitoring program compliance by DDOs
    ● Add bullet: ensuring records that contain personally identifiable information are maintained securely throughout their lifetime
    ● Revise bullet: training, assisting and consulting with department offices on records management methods, practices and requirements

◆ Section 2, subsection Responsibilities of Districts, Divisions, and Offices
  ● Districts, divisions and offices are responsible for….  
    ● Add bullet: developing and maintaining office or work unit file plans

◆ Section 2, subsection Employees with Specific Responsibilities
  ● Revise descriptions to include oversight, monitoring and file plan development and maintenance responsibilities for DDO Records Administrators, Custodians and Coordinators.

Chapter 2, Record Copy Responsibility:

◆ Section 3, revise reference to General Services Division (GSD) to Procurement Division for example figure.
Chapter 4, File Management:

- Section 4, subsection **Definition and Content**
  - Add: All TxDOT offices or work units are required to develop and maintain a file plan. Records custodians must certify the currency and accuracy of their file plans to the DDO Records Administrator, who, in turn must certify the currency and accuracy of their organization's file plan to TxDOT Records Management.
  - File plans must be reviewed and revised as necessary to maintain their utility for locating files.
  - Add reference to standard file plan in an Excel spread sheet. Revise descriptive table to include all fields in standard Excel file plan and provide instructions for cutting and pasting shared drive folder structure into the file plan. Insert new figure illustrating the file plan spreadsheet.

- Section 4, add new subsection **Certification**

Chapter 5, Electronic Records:

- Section 3, subsection **Retaining Electronic Records**
  - delete reference to GroupWise email.

- Section 4, subsection **Classifying Email**
  - Revise bullet in-line title from Operational email to Transaction-Related email.

- Section 4, subsection **Capturing Email for Retention**
  - Delete sentence "The GroupWise tool bar allows users the option of saving messages directly to the FileNet EDMS."
  - Delete "Saving an email message as a document ("save as" to a shared drive or adding to the EDMS) does not preserve more detailed metadata showing the receipt and disposition of the email. It may also result in the loss of formatting of tables, lists, and other email content. However, saving email in this manner...." and revise paragraph to read: "Saving an email message as a document ("save as" to a shared drive or adding to the EDMS) is acceptable as a routine business practice, as it preserves the basic content of the record and the essential properties of sender, recipient and date."

- Section 6, subsection **Email Best Practices**
  - Revise reference to TSD web site to IT.

Chapter 10, Records Destruction:

- Section 2, subsection **Destruction of Records Stored Locally**
  - Insert procedure table describing procedure for coordination and Records administrator review and approval process for destruction of locally retained records.
Contact

For additional information or to recommend improvements to this manual, please contact Records Management by email at GSD_Records_Management@txdot.gov.

Archives

Past manual notices are available in a pdf archive.
# Table of Contents

## Chapter 1 — Program Overview

Section 1 — Introduction. ................................................................. 1-2  
Legal Requirement and Program Authority ........................................ 1-2  
Definition of Record ........................................................................ 1-2  
Essential (Vital) Records. ............................................................... 1-3  
Other Definitions. ........................................................................... 1-3  

Section 2 — Program Objectives, Scope, Roles, and Responsibilities .......... 1-4  
Program Objectives ........................................................................ 1-4  
Program Scope ................................................................................ 1-4  
Program Responsibilities. ............................................................... 1-4  
Responsibilities of Districts, Divisions, and Offices. ............................. 1-5  
Employees with Specific Responsibilities .......................................... 1-5  
Contact Information ........................................................................ 1-6  

## Chapter 2 — Record Copy Responsibility

Section 1 — The Record Copy Concept ............................................... 2-2  
Record Copy Definition .................................................................... 2-2  
Characteristics of a Record Copy ...................................................... 2-2  
Electronic Records and the Record Copy Concept ............................... 2-2  

Section 2 — Record Copy Responsibility .......................................... 2-3  
Definition ......................................................................................... 2-3  
Determining Responsibility. ............................................................ 2-3  
Coordinating Responsibility ............................................................. 2-3  
Records Retention Policy ................................................................. 2-3  

Section 3 — Record Copy Responsibility Lists .................................. 2-5  
Defining and Using the List ............................................................... 2-5  
List Structure .................................................................................... 2-5  

## Chapter 3 — Records Retention Schedule

Section 1 — Purpose and Responsibilities ......................................... 3-2  
Purpose ............................................................................................ 3-2  
Responsibilities .............................................................................. 3-2  

Section 2 — Description and Organization ....................................... 3-3  
Description ....................................................................................... 3-3  
Organization .................................................................................... 3-3  

Section 3 — Schedule Contents ....................................................... 3-4  

Section 4 — Amending the Schedule ............................................... 3-6
Chapter 4 — File Management

Section 1 — Organizing Files ............................................. 4-2
  Overview and General Principles ................................... 4-2
  Organizing for Retrieval ............................................. 4-2
  Basic Arrangements .................................................. 4-2
  Hierarchical Groupings .............................................. 4-2

Section 2 — File Management on Shared Drives ....................... 4-4
  File Location .......................................................... 4-4
  File Naming and Organization ..................................... 4-4
  Date-Based File Organization ...................................... 4-4
  Event-Based File Organization .................................... 4-5
  Document Naming .................................................... 4-5
  E-mail Guidelines ..................................................... 4-6

Section 3 — File Management in an EDMS .............................. 4-8
  Active and Passive EDMS Uses ..................................... 4-8
  EDMS and SharePoint Services ..................................... 4-8
  Using Properties to Manage Files in an EDMS .................... 4-8
  EDMS File Management Procedural Overview ..................... 4-9
  Declaring a Record .................................................. 4-10
  Securing the Record ................................................. 4-10
  Including EDMS in Periodic Records Management Procedures .... 4-10
  Reporting Records to be Destroyed ................................. 4-11
  Deleting the Records ................................................ 4-11
  Using the File Code Property ....................................... 4-11
  Controlling EDMS Costs ............................................. 4-12

Section 4 — Using a File Plan ............................................ 4-13
  Definition and Content .............................................. 4-13
  Certification ........................................................... 4-15
  Distributing the File Plan ......................................... 4-16
  Support for Discovery and Open Records .......................... 4-16

Section 5 — Hard Copy File Management ............................... 4-17
  Visual Techniques .................................................... 4-17
  File Coding ........................................................... 4-17
Organizing and Labeling File Folders and Guides .......................... 4-18
Setting Up Files ................................................................. 4-19
Preparing File Guides .......................................................... 4-19
Preparing Folder Labels ....................................................... 4-19
Preparing File Drawer Labels ............................................... 4-20
Coding Records for Filing ..................................................... 4-20
Cross-References ............................................................... 4-20
Charge-Out Records ............................................................ 4-21
Problems in File Organization ............................................... 4-21
Section 6 — Conducting Routine File Closing Procedures ................. 4-22
Benefits ........................................................................... 4-22
Establishing a Routine .......................................................... 4-22
Coordinating Procedures ...................................................... 4-22
Purging Procedures ............................................................ 4-23

Chapter 5 — Electronic Records
Section 1 — Definition and Overview ........................................ 5-2
Definition of Electronic Record ................................................. 5-2
Chapter Overview ............................................................... 5-2
Section 2 — Requirements for Managing Electronic Records .......... 5-3
Introduction ........................................................................ 5-3
Section 3 — General Practices for Managing Electronic Records .... 5-4
Working Files and Record Copies .............................................. 5-4
Retaining Electronic Records ................................................. 5-4
Using Offline Media .............................................................. 5-4
Maintaining Offline Media ..................................................... 5-5
Protecting Record Integrity ..................................................... 5-5
Securing Confidential Records ................................................. 5-6
Document Imaging ............................................................... 5-6
Requirements and Recommendations for Imaged Records .......... 5-7
Destruction of Electronic Records .............................................. 5-14
Section 4 — Managing Email Records ........................................ 5-15
Managing Email Records ....................................................... 5-15
Classifying Email ............................................................... 5-15
Employee Training .............................................................. 5-16
Content Templates and Naming Conventions ......................... 5-16
Capturing Email for Retention .............................................. 5-16
Section 5 — Records Management in an EDMS ............................ 5-18
Introduction ........................................................................ 5-18
Ownership Responsibility and Authority ........................................... 5-18
Identifying Record Types ................................................................. 5-18
Selecting Documents to Add ............................................................. 5-19
Managing Drafts or Versions ........................................................... 5-19
Declaring a Record ........................................................................ 5-19
Retaining Hard Copy Originals after Scanning .................................. 5-20
Document Signature Considerations ................................................ 5-20
Evaluating Archival Needs ............................................................... 5-20
State Archives Requirements .......................................................... 5-21
Documenting Procedures ................................................................. 5-21
Records Management Procedures in an EDMS .................................. 5-21
Section 6 — Risk Management and Electronic Records ...................... 5-23
Legal Use of Electronic Records ....................................................... 5-23
Email Best Practices ...................................................................... 5-24
Preparing for Electronic Discovery .................................................. 5-25

Chapter 6 — Vital Records
Section 1 — Identifying Vital Records ............................................... 6-2
Vital Records ................................................................................ 6-2
Identifying Vital Records ................................................................. 6-2
Responsibility for Vital Records ....................................................... 6-2
Common Vital Records .................................................................. 6-3
Section 2 — Threats and Protection .................................................. 6-5
Introduction .................................................................................. 6-5
Potential Threats to Records ............................................................ 6-5
Methods of Records Protection ....................................................... 6-6
Storage Equipment and Conditions ................................................ 6-7

Chapter 7 — Disaster Recovery Planning
Section 1 — Overview ..................................................................... 7-2
General -- Steps in Disaster Recovery Planning ................................. 7-2
Definitions .................................................................................... 7-2
Section 2 — Disaster Prevention ...................................................... 7-3
Recognizing Threats to Records ..................................................... 7-3
Methods of Protection ................................................................... 7-4
Section 3 — Developing a Disaster Recovery Plan .............................. 7-6
General -- What the Plan Involves .................................................... 7-6
Emergency Supplies and Services .................................................. 7-6
Disaster Recovery Team ................................................................. 7-6
Recovery Team Responsibilities ...................................................... 7-7
Chapter 8 — Inactive Record Storage

Section 1 — Overview
Introduction
Records Eligible for Storage at a Records Center
Storage Locations
Selecting Records for Storage

Section 2 — Transferring Records to Storage
Procedural Overview
Division and Office Procedure
Proper Packaging and Documentation

Section 3 — Transmittal and Storage Documentation
Uses of Form 1419, Records Transmittal
Instructions for Completing Form 1419

Section 4 — Receipt and Storage Location
Receipt Procedures

Section 5 — Retrieving Records
Procedure
Monitoring of Checked-Out Records

Section 6 — Storage Areas and Equipment
Introduction
Essential Requirements for Storage Areas
Record Location Aids
Types of Storage Boxes

Chapter 9 — Microfilming Records

Section 1 — Overview
Archival Records in an EDMS ................................. 10-13
Chapter 1 — Program Overview

Contents:

Section 1 — Introduction

Section 2 — Program Objectives, Scope, Roles, and Responsibilities
Section 1 — Introduction

Legal Requirement and Program Authority

The Texas Government Code, Chapter 441.183 et. seq., requires state agencies to establish and maintain a records management program on a continuing and active basis. Specific rules related to managing state records are published in the Texas Administrative Code, Title 13, Chapter 6. The Records Management site on the department's intranet contains links to statutes and rules that govern the operation of TxDOT's records management program.

Each agency head is responsible for the proper management of state records and is required to appoint a records management officer to administer the agency's records management program.

Administrative Order 4-77 assigned responsibility for the department's records management program to the Equipment and Procurement Division, now known as the Enterprise Content and Records Management, (ECRM). The Records Management Unit in ECRM has overall responsibility to develop and manage TxDOT's records management program. Each district, division and office is responsible for implementing the program internally.

Definition of Record

A record (or file) is composed of single or multiple documents, books, papers, photographs, computer-generated or stored data, videos, sound recordings, or other materials, regardless of physical qualities, that are made or received by a state department or institution according to law or in connection with official state business. (§441.180(11) Government Code).

This manual uses the terms file and record interchangeably and generically, as distinguished from their uses relating to objects in electronic data management terminology.

CAUTION: Any document produced in state facilities on state equipment may be considered a state record by the courts. This also applies to any document related to state business that exists on personal equipment, such as an employee's home computer. Also, a duplicate copy of a document becomes a record by default if it replaces an original that has been lost or destroyed.

The following are not records:

- library or museum material made or acquired and preserved solely for reference or exhibition
- an extra copy of a document kept only for reference, a stock of publications or processed documents, or
- any records, correspondence, notes, memoranda, or other documents associated with a matter conducted under an alternative dispute resolution procedure in which personnel of a state
department participated as a party, facilitated as an impartial third party, or facilitated as the administrator of a dispute resolution system or organization.

A duplicate (convenience, information or reference) copy of a document may become a record by default if it replaces an original that has been lost or destroyed.

**Essential (Vital) Records**

A vital record is a record that is necessary for TxDOT to do any of the following after a disaster:

- resume or continue operations,
- reaffirm authority and activity, including legal and financial positions, and/or
- protect the rights and interests of the department and its customers.

[Chapter 6](#), “Vital Records,” discusses procedures to protect vital records.

**Other Definitions**

A **document** is a vehicle for conveying information or content, in either hard copy or electronic media.

The document or record **life cycle** refers to the stages of document creation, active use, inactive retention/storage and final disposition.

The **retention period** is the period of time a record must be retained before it becomes eligible for destruction. Minimum retention periods may be required by law, organizational policy, or business process needs.

Additional terms are defined in chapters related to specific topics.
Section 2 — Program Objectives, Scope, Roles, and Responsibilities

Program Objectives

Records management consists of policies and procedures intended to
◆ ensure compliance with state records management laws and requirements,
◆ reduce costs for maintaining state records, and
◆ manage risks related to records.

In addition to assuring legal compliance, records management reduces costs for physical and electronic record keeping resources by controlling volumes and promoting efficient organization and management of active and inactive files for retrieval.

Risk Management. Records management helps manage legal risks that can result from maintaining outdated records. An approved records retention schedule provides legal authority to destroy records when their required retention period has been met.

Program Scope

The scope of TxDOT’s records management program includes
◆ developing and maintaining a records retention schedule approved by the State Auditor and the Texas State Library,
◆ developing and publishing records management procedures,
◆ developing and disseminating procedures for protecting vital TxDOT records,
◆ providing guidance and assistance to help department offices manage records efficiently and in compliance with the requirements of statute and department policy,
◆ coordinating the retention and disposition of official TxDOT records in accordance with approved retention policy.

Program Responsibilities

The Records Management program is responsible for
◆ researching, developing and recommending records management policies to management;
◆ ensuring records that contain personally identifiable information are maintained securely throughout their lifetime,
◆ maintaining a current, approved records retention schedule,
◆ oversight and monitoring program compliance by DDOs,
◆ coordinating TxDOT's records management program with outside agencies as required;
◆ maintaining current procedures in the Records Management Manual and disseminating program information on the Intranet;
◆ training, assisting and consulting with department offices on records management methods, practices and requirements;
◆ managing records storage for headquarters divisions and offices; and
◆ maintaining required program records.

**Responsibilities of Districts, Divisions, and Offices**

Districts, divisions, and offices are responsible for
◆ compliance with TxDOT records management policies, and
◆ implementing TxDOT records management procedures, including
  • developing and maintaining office or work unit file plans,
  • identifying vital records and taking measures to protect them;
  • retaining official state records for the required retention period, whether locally or in remote storage facilities; and
  • coordinating the timely destruction of records when they become eligible and submitting required record destruction documentation to TxDOT records management.

**Employees with Specific Responsibilities**

The **TxDOT Records Management Officer** is designated by the executive director as the TxDOT records management officer for coordinating the program with the Texas State Library and is responsible for program oversight, maintaining compliance with requirements of Government Code §441.183 et. seq. and 13TAC §6, development and management of standardized internal procedures to support agency-wide access to and compliant retention and preservation of records, DDO program compliance monitoring and reporting, and consultation and development of ongoing records management training.

DDO **Records administrators** are appointed by district engineers, division, and office directors to implement and manage the records management program in their respective organizations, to include development and maintenance of work unit file plans, coordination and management of routine periodic procedures to monitor, certify and repost currency of file plans, verify records being
records retained, and authorization and documentation of the destruction of eligible records by records custodians.

Records Custodians are managers or supervisors knowledgeable of, and responsible for, the official records related to their functional areas or work units/offices. While custodians may delegate record keeping tasks to Records Coordinators (or perform Records Coordinator duties themselves), they are responsible for ensuring and certifying the currency and accuracy of their work unit file plans, verifying that their records are being retained appropriately, and reviewing, authorizing and documenting destruction of their records when they become eligible.

Records Coordinators are employees who perform record keeping tasks under the direction of the Records Custodian, such as physical or digital file management, preparation and updating the work unit file plan, coordinating and managing records storage, monitoring and reporting records eligible for destruction, overseeing destruction and/or completion of the Form 1420, Records Destruction Log for Custodian approval and signature.

Contact Information

Current contact information is available on the Intranet.
Chapter 2 — Record Copy Responsibility

Contents:

Section 1 — The Record Copy Concept
Section 2 — Record Copy Responsibility
Section 3 — Record Copy Responsibility Lists
Chapter 2 — Record Copy Responsibility  Section 1 — The Record Copy Concept

Record Copy Definition

The record copy is the official record that must be retained to fulfill statutory retention requirements. Convenience or “information” copies are duplicates of the record. They are not subject to retention requirements and may be destroyed without formality when they are no longer needed. Convenience copies retained beyond the retention period approved for the record copy become the record copy by default and remain subject to legal and open records demands.

Characteristics of a Record Copy

A record or file is usually a record copy when

◆ it is the original record or file; it may or may not bear an original signature;
◆ it originates or is retained at the office responsible for the operation or function the record or file concerns;
◆ it was originally a convenience, information or other non-record copy to which significant annotations or signatures have been added; and/or
◆ it was originally a convenience or information copy, but has been retained past the destruction of the original record copy becoming by default the record copy.

It is possible for the same document to be present in two or more units of the agency and be the record copy in each unit if it serves a different function in those units. When in doubt about the status of a record, it is safest to handle it as a record copy.

Electronic Records and the Record Copy Concept

Records may be created and maintained electronically without ever being produced in hard copy. It is important to determine the final content of the official electronic record and to institute procedures to dispose of working copies, drafts and duplicates when the final record is complete. Because of the ease with which electronic records can be copied and shared, the presence of copies represents a particular vulnerability to the organization.

Chapter 4, File Management, offers procedures that support management of electronic records.

An enterprise document management system (EDMS) addresses vulnerabilities associated with duplicate electronic records. When implementing and developing an EDMS, it is critical to determine and coordinate record copy responsibility.
Section 2 — Record Copy Responsibility

Definition

Record copy responsibility refers to the responsibility for maintaining the official copy of a TxDOT record in accordance with the retention policy in the agency's records retention schedule. Specific organizational units in districts, divisions and offices typically have responsibility for the creation, maintenance and retention of official records related to their functions.

Determining Responsibility

Typically, the office that creates the record, or has primary responsibility for operations related to the record, or that performs the final action on a form, document or other record, is the office with record copy responsibility. This is particularly the case when an office has "sign-off" or approval responsibility related to a function documented in the files and the office is responsible for maintaining the official file.

Consider the relationship of the file to the office’s function. Files related to an office's function often contain mixed original records and convenience copies. Some duplication is inevitable. It is unnecessary and impractical to micromanage files on a document by document basis. The best practice in this circumstance is to treat the file as a record copy and manage it accordingly.

Coordinating Responsibility

To clarify responsibility for retaining records and to reduce file management overhead in other offices, business process managers should coordinate record copy responsibility between department offices. This is especially important when using an enterprise document management system (EDMS), as only a single document (the record copy) in the appropriate repository is required for retention. System security management determines who in the enterprise can or cannot access or modify the document.

Besides management functions, EDMS provides the added benefit of reducing storage space, equipment, and associated costs.

Records Retention Policy

The TxDOT records retention schedule defines the required minimum retention period for record copies. The responsible office must retain the record for the required retention period listed in the TxDOT records retention schedule, whether the record is kept in the office or in storage. (NOTE: Records Management does not accept non-record copies from divisions and offices for storage.)
The record custodian in that office is responsible for approving and documenting the destruction of the records.
Defining and Using the List

A record copy responsibility list identifies the office(s) responsible for specific records. Besides reducing redundant record keeping, the list helps coordinate the disposition of convenience copies when record copies are destroyed. The list can also help locate records or documents subject to legal holds or open records requests.

A record copy responsibility list template based on the current records retention schedule for common records is downloadable from the Records Management intranet site. It may be edited as necessary to meet individual district or division requirements. Posting a link on a district, division, office, or region (D/D/O) intranet site is an efficient method of dissemination.

List Structure

The record copy responsibility list contains sufficient information from the records retention schedule to identify records management requirements, and provides a column identifying the office responsible for the record copy. The table following the example describes information in the columns on the list.

<table>
<thead>
<tr>
<th>Agency Item Number</th>
<th>Record Series Title</th>
<th>Ret. Period</th>
<th>Remarks</th>
<th>Responsible Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROW07</td>
<td>Sign Permit Files: Records related to advertising sign permits, including renewals, transfers, and fees collected.</td>
<td>AC+3</td>
<td>AC = Expiration/ termination of permit. VITAL RECORD.</td>
<td>District ROW</td>
</tr>
</tbody>
</table>

Record Copy Responsibility List Field Descriptions

<table>
<thead>
<tr>
<th>Block</th>
<th>Description</th>
</tr>
</thead>
</table>
### Record Copy Responsibility List Field Descriptions

<table>
<thead>
<tr>
<th>Block</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Office</td>
<td>Identifies the office(s) within the district that maintains the record copy. It may be convenient to complete this block for exceptions only. For district accounting records (ACC) that are maintained by the district accounting office, you may choose to leave the block blank. If the particular accounting records are maintained by another office, fill the block in. There will be instances where all offices have responsibility for certain types of records, such as general correspondence.</td>
</tr>
</tbody>
</table>
Chapter 3 — Records Retention Schedule

Contents:

Section 1 — Purpose and Responsibilities
Section 2 — Description and Organization
Section 3 — Schedule Contents
Section 4 — Amending the Schedule
Section 5 — Records Inventory
Section 1 — Purpose and Responsibilities

Purpose

In accordance with Texas Government Code §441.185, TxDOT maintains a records retention schedule approved by the Texas State Library and Archives Commission. The schedule documents TxDOT records retention policy and is based on requirements in federal and state statutes, rules and regulations, and requirements established by department offices.

An approved records retention schedule

- fulfills requirements of state law and department policy;
- secures TxDOT’s statutory authority to retain, store and dispose of department records;
- guides districts, divisions and offices on the minimum retention requirements for record copies; and
- documents TxDOT’s business practice regarding records retention, and
- must be recertified by the Texas State Library and Archives Commission every five years.

The current, approved TxDOT records retention schedule is posted on the records management intranet page.

Responsibilities

The TxDOT records management officer has overall responsibility for developing and maintaining the records retention schedule and coordinating its periodic recertification.

Records administrators coordinate records management in districts, divisions and offices. They are responsible for helping their organizations to implement the records retention schedule and coordinating revisions to the schedule when necessary.

Records coordinators and custodians manage records in specific offices or units of districts, divisions and offices and implement the records retention schedule in their file management activities. They may also make recommendations on revisions to the records retention schedule.
Section 2 — Description and Organization

Description

The records retention schedule, available to employees on the Records Management intranet site, lists TxDOT records and specifies the minimum period of time they must be kept before being eligible for destruction. An approved schedule provides the agency with the authority to manage state records and destroy them when their required retention period expires.

Organization

The records retention schedule consists of two parts.

The first part lists record series common to all TxDOT districts, divisions and offices and includes types of records related to accounting; administrative; administrative operational; information resources; personnel and safety records; and records series related to specific district operations. The common schedule is inclusive. Not all offices have all record series, but may refer to the guidance in the common schedule for those records they have.

The second part of the schedule lists unique record series maintained by specific divisions and offices.
Section 3 — Schedule Contents

Figure 1 shows the Texas State Library and Archives Commission's State of Texas Records Retention Schedule, Form SLR 105, currently used to document TxDOT records retention policy.

![Records Retention Schedule](image)

The contents of the schedule include:

- **the Record Series Item Number** - a reference to specific types of records on the State of Texas Records Retention Schedule (13 TAC §6.10). The first two digits identify groupings of...
categories of records. For example, 3.1 refers to employee records. If a record series item number consisting of five digits appears, the record series is specifically identified in the state schedule;

- the **Agency Item Number** - a location reference on the TxDOT records retention schedule used for indexing and citation of official state records described in the schedule. The elements of this number are:
  - a functional account number of the district, division or office responsible for the record,
  - a three-letter acronym describing the type of record or the responsible office, and
  - a number indicating the sequence of the record series in the schedule.

For example, the agency item number 44ADM04 indicates that the records referred to are from the **Procurement** Division (functional account number 44) and the records are described fourth in the list of administrative records on the schedule.

- The **Record Series Title** - describes the type of record, which may consist of a single specific type of record or file or a group of files that are similar in function and have similar retention requirements.

- The **Retention Period** columns - describe the minimum amount of time the record copy must be retained before it becomes eligible for destruction.
  - **Agency**: Length of time records retained in TxDOT
  - **Storage**: Length of time records may be stored at the State Records Center. TxDOT does not currently store records at the State Records Center, and does not use this column
  - **Total**: A code that describes how long the official (record copy) records must be retained

For example, FE+3 means records must be retained until the end of the fiscal year plus three years, becoming eligible for destruction after September 1 of the third year of its retention.

- The **Archival Code** - indicates requirements for records to be deposited or reviewed by the State Archives before destruction.

- The **Remarks** - are for additional information such as special retention requirements, legal citations related to retention, handling for imaging, etc.

- The **106 Number** - refers to a form used by the State Records Center (SRC) for records that are stored at that facility.
Section 4 — Amending the Schedule

Amending Existing Entries

Changes in legal or regulatory requirements, functions, organization, or business requirements may necessitate an amendment to the records retention schedule. To initiate the process, business area experts should recommend needed amendments to the schedule to the TxDOT records management officer through their respective administrators. The TxDOT records management officer monitors organization and functional operations, and may also recommend necessary amendments.

Amendments are documented on a Form SLR 122.
Adding New Records Series

When developing a new type of record or file, first review the schedule to see if it matches an existing record series description. If a match is not apparent, contact the TxDOT records management
officer, who may be able to relate the new records to an existing record series.

If a new record series must be added, the records coordinator or custodian completes Form RMD103, Records Inventory Worksheet to furnish descriptive documentation supporting the addition of an official record series to the schedule, and forwards it through the records administrator to the records management officer.

A Records Inventory Worksheet is not necessary when

- the record series matches a record series on the TxDOT records retention schedule;
- the record series is a new record or file in an existing record series listed on the records retention schedule, and the record series title is still appropriate (if you think the existing title needs to be revised, contact the records management officer);
- the retention period or minor changes in the characteristics of the records for an existing record series is changing. (You can coordinate this change by e-mail or memo with the records management officer.)

Coordination and Approval of Amendments

The TxDOT records management officer drafts the amendment and coordinates the change with the requesting records administrator. The records management officer may coordinate amendments for any related records with other offices that may be affected, and submits the amendment to the Texas State Library and Archives Commission for approval.

Upon approval, the records management officer advises the records administrator and posts the amended schedule, an updated list of changes and any necessary revision to the Record Copy Responsibility List template to the records retention schedule published on the intranet.
Section 5 — Records Inventory

The records inventory provides significant facts about the records a work unit creates and maintains. Although a department wide inventory was conducted for the initial development of the records management program, work units should conduct periodic reviews to maintain current records inventory information through changes in function, organizational placement and record keeping technology.

Records Inventory Worksheet

Form RMD103, Records Inventory Worksheet, captures records inventory information to document the existence and requirements for managing official records series.
The inventory worksheet is divided into two parts. The person conducting the inventory completes the inventory section (items 1 to 21), in which each records series is located, identified, and described. The records management officer completes the appraisal section (items 22 to 24) to transfer to the records retention schedule.
Some fields will not apply to the records being examined. The worksheet can be tailored to meet the needs of the work unit, and it is only necessary to complete the fields where the information applies. The following table describes the information to entered on the worksheet.

**Completing a Records Inventory Worksheet**

<table>
<thead>
<tr>
<th>Block Number</th>
<th>Content</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 5</td>
<td></td>
<td>Self-explanatory.</td>
</tr>
<tr>
<td>6</td>
<td>Working Records Series Title</td>
<td>Enter a working record series title. A records series is a group of identical or related documents arranged under a single filing system or kept together as a unit because they relate to the same subject, result from the same activity, or document the same transaction, and which, because of any of these common characteristics, may be treated as a unit for retention and disposition purposes. A records series is determined by the function and the retention of the record, not by filing considerations or by format. You can use existing listings on the TxDOT records retention schedule as a guide</td>
</tr>
<tr>
<td>7</td>
<td>Description</td>
<td>Describe the record or file in clear and simple terms that someone unfamiliar with the records can understand. Spell out acronyms. Describe the contents or purpose of forms. Make the description as complete as possible so the records management officer can understand the nature of the record or file.</td>
</tr>
<tr>
<td>8</td>
<td>Status</td>
<td>Mark the appropriate box. Only record copies require completion of a worksheet. If there is any doubt about record copy status, discuss the records with the records management officer who will help you determine record copy status.</td>
</tr>
<tr>
<td>9</td>
<td>Record Medium</td>
<td>Specify the medium of the record or file. You may specify more than one medium. If records are maintained in hard copy for a period of time and then imaged, indicate how long they are kept before imaging and what happens to the hard copy originals afterwards. If only certain records in a record series are imaged, indicate which ones.</td>
</tr>
<tr>
<td>10</td>
<td>Arrangement</td>
<td>Describe how the record or file is arranged or ordered. If arranged by more than one element, specify the elements (i.e., alphabetically by fiscal year).</td>
</tr>
<tr>
<td>11</td>
<td>Volume</td>
<td>State volume in cubic feet. A standard file drawer is 1.6 cubic feet; a standard document storage box is 1 cubic foot. Include active and inactive (stored) records.</td>
</tr>
<tr>
<td>12</td>
<td>Estimated Activity</td>
<td>Estimate the amount of records activity (frequency of access and retrieval).</td>
</tr>
</tbody>
</table>
### Completing a Records Inventory Worksheet

<table>
<thead>
<tr>
<th>Block Number</th>
<th>Content</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Restrictions</td>
<td>Check off the applicable restrictions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Legal: Cite any legal or regulatory requirement related to management or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>retention of the record.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Vital: Is the record vital (essential)? Before checking this box, see</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chapter 6, “Vital Records.” Special handling requirements apply to vital</td>
</tr>
<tr>
<td></td>
<td></td>
<td>records.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Confidential: Records may contain information that requires confidential</td>
</tr>
<tr>
<td></td>
<td></td>
<td>handling. Labeling records confidential does not necessarily affect their</td>
</tr>
<tr>
<td></td>
<td></td>
<td>status under the Public Information (Open Records) Act, Government Code,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>§552.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Archival: Certain records must be deposited with the State Archives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The State Archives must review other records before they may be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destroyed. The records management officer will research archival status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Subject to Audit: Certain records are subject to internal or external</td>
</tr>
<tr>
<td></td>
<td></td>
<td>audits. Before these records can be destroyed, the records coordinator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and records administrator must certify that audit requirements have been</td>
</tr>
<tr>
<td></td>
<td></td>
<td>met.</td>
</tr>
<tr>
<td>14</td>
<td>Storage</td>
<td>Specify how records are stored.</td>
</tr>
<tr>
<td>15</td>
<td>Current Retention Period</td>
<td>Enter a tentative retention period. Most records do not need to be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>retained longer than three or four years. If there is a reason to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>retain the records longer, write a brief explanation on the back of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>worksheet. The records management officer will research retention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requirements and advise on any special requirements related to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>record series. Permanent retention requires written justification if the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>record series does not have a permanent retention requirement in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>State of Texas Records retention schedule. Use the back of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>worksheet. Records approved for permanent retention should be stored in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>an imaged format, unless law requires retention of the original hard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>copy.</td>
</tr>
<tr>
<td>16</td>
<td>Inclusive Dates</td>
<td>Specify dates for both active and inactive (stored) records or files.</td>
</tr>
<tr>
<td>17 – 21</td>
<td></td>
<td>Self-explanatory.</td>
</tr>
<tr>
<td>22 – 24</td>
<td></td>
<td>The TxDOT records management officer completes these blocks.</td>
</tr>
</tbody>
</table>
Chapter 4 — File Management

Contents:

Section 1 — Organizing Files
Section 2 — File Management on Shared Drives
Section 3 — File Management in an EDMS
Section 4 — Using a File Plan
Section 5 — Hard Copy File Management
Section 6 — Conducting Routine File Closing Procedures
Section 1 — Organizing Files

Overview and General Principles

Most department offices already have organized file arrangements or file plans in place for hard copy records. This chapter addresses general file organizational principles to employ when the need arises to

- create, revise or overhaul a filing system;
- develop and apply file management techniques and procedures to electronic documents and records;
- develop or revise a file plan index to files; or
- establish procedures to review files in all media for storage and disposition.

The principles apply to files in any medium.

Organizing for Retrieval

Organize files for easy and intuitive retrieval of information. Organization is typically hierarchical, moving from broad categories through subcategories to specific contents such as individual folders or documents. The usual need is to retrieve a specific document. In hard copy file systems organization through the folder level is ordinarily sufficient. In an electronic file system organization techniques may extend to specific criteria to identify individual documents.

Proper organization enables both efficient retrieval of individual documents and the efficient management of the record series to which they belong through the record life cycle.

Basic Arrangements

The three basic types of file arrangement are

- **alphabetical** - using names, subjects, geographic locations, etc.;
- **numerical** – using numbers in various combinations, such as date, control-section and job, etc.; and
- **alphanumerical** – using a combination of letters and numbers.

Hierarchical Groupings

Typical file organization moves from broad groupings of files through progressively more specific groupings to particular files or documents.
Major Groups - A major group is a broad grouping of files related to major functions or areas of activity. Major groups vary according to the function of the individual organizational unit maintaining the files.

Minor Groups - Minor groups consist of different files that relate to similar types of activity or function. For example, the following minor groups may exist as folders under the major group of Office Administration: Budget files, Material Issues and Purchasing files, and Annual Equipment Inventory files.

Component Files or Folders – Component files or folders consist of assemblies of documents related to a particular subject, event, function or transaction. These may include sub-folders under folders or documents within an individual folder.
Section 2 — File Management on Shared Drives

File Location

Use shared drives to maintain electronic files enhances accessibility and security. Standard procedures should include guidance to employees on routine transfers of electronic files from individual desktops to the shared drive as they are developed in the course of business functions.

While shared drives offer convenience when documents are being developed, the FileNet enterprise document management system (EDMS) is the preferred repository for the retention of completed documents. Until EDMS is fully implemented across the enterprise, however, many offices will continue to maintain electronic records on their shared drives.

This section discusses addresses the following techniques for managing files on the share drive:

- file Naming and Organization
- date-Based File Organization
- event-Based File Organization
- document Naming
- e-mail Guidelines

File Naming and Organization

Electronic file naming should support both retrieval and record life cycle management for electronic files that are retained on a shared drive. While document and folder names may suggest content, use of dates or numbers in the names can help to graphically organize them on the display.

Date-Based File Organization

Organize and name date-managed files in the following manner:
Event-Based File Organization

Employ the same folder structure as the date-based arrangement, above, but create separate folders to contain active and completed files, as in the following example:

- **Major Group Name (Project type or component, for example)**
  - **Active Projects (Minor Group)**
    - **County**
      - **CSJ**
  - **Completed CY or FY 20## (Minor Group)**
    - **County**
      - **CSJ**

As the status of records changes from active to completed, move the records from the Active minor group to the appropriate folder in the Completed Minor Group.

Since records are typically managed on a periodic basis, organization of completed event-based records by year of completion is ordinarily sufficient to accomplish efficient retention and destruction of records. Folder structures can be organized for a closer adherence to minimum retention requirements for sensitive records by using month folders, or a similar finer level of detail in a date-based minor group.

Document Naming

Appropriate document naming is essential to allow accurate identification of content for retrieval. In most functions, using a combination of a date and standard title suggestive of the document content or function is sufficient. Document naming conventions can be established as routine procedures for many documents related to operations. Some examples include the following:
File Management on Shared Drives

- MM-DD-YY Approval Memo (or E-mail or Letter or Form) (NOTE: It may be helpful for retrieval to include the type of document format, such as e-mail or form, for correspondence.)
- MM-DD-YY Status Report (File suffix (.doc, .xls,) will identify type of document)
- MM-DD-YY (Recipient Name) E-mail
- MM-DD-YY Form Title-Person Name or other Identifier

Use of the date allows for an easy sequential organization of documents related to a process. Numerical suffixes can identify consecutive content related to a document or subject.

Managers or supervisors can establish naming conventions appropriate to the needs of their operations and train employees to use them.

CAUTION: Excessively long folder or document names may result in file corruption that prevents document actions, such as moving or copying document files.

E-mail Guidelines

E-mail messages created or received by means of state resources, including employees and facilities, are considered state records. Inadequately managed or controlled e-mail represents a significant legal vulnerability in most organizations. While users may view the medium as a communications utility, much like the telephone, the courts may consider e-mail messages as documentary evidence. Responsibility for appropriate management of e-mail is shared by managers, supervisors and users.

Basic Guidelines. Several basic measures can reduce risks related to e-mail, including the following:

- identifying and characterizing e-mail related to routine business functions
- developing e-mail subject/naming conventions to relate the content to a specific record
- developing e-mail text templates for use in routine business communications
- establishing and enforcing procedures to save e-mail to the appropriate record folder immediately upon completion of the transaction
- arranging for frequent and regular automatic emptying of mailboxes
- training employees on e-mail procedures and include appropriate e-mail management in performance planning and evaluation
- copying only those who have a direct stake in the content of the e-mail
- using links to documents posted to the intranet for broadcast e-mail communications
**Record Copy Status.** Identify and retain e-mail according to the requirements for the record to which its content relates. The following guidelines can help in determining the record copy status of e-mail:

- The person authoring an e-mail in connection with a business function may be presumed to have created the original (e-mail) record
- E-mail that contains a string of dialog, (initial message, response(s), and attachments) that represents a completed communication or transaction related to a function for which the office or unit is responsible is normally a record.

Transitory e-mail typically not considered for record copy status includes:

- e-mail received that does not require a response or further documented action;
- e-mail transmitting attachments (unless it is important to retain documentation of the transmission itself);
- informal conversational e-mail that does not include content that turns the message into a record.

**Saving to the Shared Drive.** Saving e-mail to the appropriate folder on the shared drive as a routine procedure related to the maintenance of an electronic file or record allows the content to remain accessible if the original account should be discontinued. E-mail saved in this manner defaults to a Word document in the form of a memo. The essential basic metadata of sender, recipient and date is preserved in this format.
Section 3 — File Management in an EDMS

Active and Passive EDMS Uses

Active EDMS use employs the technology to manage documents involved in the conduct of business processes. Typical actions involve coordination of revisions or document handoffs for reviews or approvals.

Passive use employs EDMS simply as a repository for retaining documents after their active use is completed. Typical actions involve adding the document or a scanned image to the library when the hard copy would ordinarily be filed.

EDMS and SharePoint Services

Microsoft’s Share Point Services (SPS) is marketed as a document management application, and has become popular as a means of sharing documents and conducting collaborative processes in the department. As documents are developed locally on shared drives, they may be posted to SPS sites for collaborative actions across the enterprise. SPS is a more user-friendly tool than FileNet for collaboration and business process-related document actions.

SPS, however, should not be used as a repository for the retention of completed documents as official records, as the ease with which SPS sites can be developed and accessed by large numbers of users and then removed presents inherent vulnerabilities. The Technology Services Division’s procedures governing the use of SPS emphasize that “SPS web sites should be focused primarily on defined projects and organizational infrastructure support issues.” Accordingly, completed or final documents managed through SharePoint should be moved to the FileNet EDMS for retention. If necessary, links to documents in the FileNet repository may be established in SPS sites.

Before eliminating SPS sites, SharePoint managers must take care to ensure that official records and documents are preserved and retained. Discussion strings may contain content necessary to preserve as a record, and steps to index and retain that content are also necessary.

Using Properties to Manage Files in an EDMS

Library developers coordinate with subject matter experts to develop indexing criteria for retrieving and managing the life cycle of documents related to their individual business processes. Users are typically unconcerned with document life cycle management after they complete their role in the process.

In an EDMS, properties, or index terms, are assigned to documents when they are added to the repository. These properties are fields in a database that is used for building searches to retrieve
documents. Documents added to the EDMS require certain properties that furnish essential data for life cycle management. These properties include the following:

- **Record Type** — Relates the document to a record series in the TxDOT Records Retention Schedule
- **Document Type** — Identifies specific document components in a record, some of which may require special retention requirements
- **Document Date** — Used for date-based purposes/document operations
- **Document Status** — Used to track document handling/life cycle status
- **File Code** — A numerical identifier used to enable batch document operations

Optional custom properties are available for document indexing to support retrieval. Ordinarily, only a limited number of index terms (or properties) are necessary for the majority of retrieval needs for documents related to a business process. It is important to establish a balance between the number of properties used and the real retrieval needs related to the document. More properties to keep track of mean greater workload in adding and maintaining documents in the repository.

Optional properties may also be used for active document management. For example, the Process Status can track a document’s relationship or use in the management of a process.

**EDMS File Management Procedural Overview**

Managers, supervisors, records custodians or coordinators must include EDMS records in routine file management procedures. The procedures resemble those for hard copy records, but involve more teamwork. The following steps are discussed in the remainder of this section:

- declaring a record to trigger retention
- changing security to preserve document integrity
- including records in the EDMS in periodic records management procedures
- generating a report of destroyed records
- deleting the records from the library

Developing queries and scripts that perform global operations on component documents of records specific to various department functions involves coordination between the OPR and EDMS system administrator. Once developed and stored, however, queries, search templates and scripts may be reused—with adjustments to certain values—to perform the same operations in the future.

**NOTE:** E-mail all queries or scripts that are based on the standard library design to EDMS_OPR@txdot.gov to ensure system users have access to these resources.
Declaring a Record

Declaring a record by an OPR may be event-driven, as in acceptance of a project, or date-driven, as in the turn of a fiscal or calendar year. For example, on notification of a construction or maintenance project’s completion, the OPR should perform a global document status property change to “Final” for all documents sharing the CSJ of the completed project. It is generally sufficient to batch records with an “AC” (After Completion) retention trigger in date-based groupings. For example, a declaration operation may specify all records with a document status of “Final” and document date equal to or before a specified trigger date, for example 0901YYYY.

The nature of the record determines its handling. If an OPR determines that a record should be destroyed as soon as it becomes eligible, it may be necessary to perform declaration and reporting on a more frequent basis.

Business process experts may collaborate with system administrators to explore developing scripts that would base global document property changes when a capstone document, such as a project acceptance letter, for example, is added to the library.

External resources may help this process. For example, the Construction Division periodically disseminates an Excel spreadsheet listing completed construction and maintenance projects by CSJ and completion dates among other categories. This data could be incorporated in scripts that run against the repository and update status properties for the affected documents.

Securing the Record

Security settings for declared records are imposed to preserve their integrity and limit access during their retention, reducing risks of inadvertent changes to, or loss of documents. It may be possible to accomplish this at the same time the record is declared.

Optimally, access to a record during retention is restricted to the EDMS system administrator. If business processes require retrieval of documents from storage, read-only access should be limited to specific individuals. To support legal inquiries concerning the integrity of records retained in the EDMS, OPRs should maintain a list of these persons, the specific record types they are authorized to access, and their rights to the documents.

Including EDMS in Periodic Records Management Procedures

Most routine procedures used to identify records eligible for destruction are managed on a date basis, typically at the turn of the fiscal year. Part of this procedure should include performing queries to report records eligible for destruction on the basis of their document status and date properties. Responsible persons then review the reports and authorize destruction of records or request withholding of destruction for specific records or documents.
In the case of reference files or documents retained indefinitely or “AV” (as long as they have administrative value) annual reviews afford owners the opportunity to reevaluate the need to retain the document.

OPRs can define the parameters of the reports. In some cases it may be sufficient to simply identify the record type and list specific identifying information, for example, denoting purchasing records for a specific fiscal year with a list of PO numbers.

Other queries may require specifying a listing that includes specific component documents.

Procedures used to report the records should include a global revision of the document status property to “Delete” and a review of documents against the EDMS file plan to identify any documents to be withheld for state archives review. Owners choosing to retain specific documents should revise the document status property to “Reference File” and enter an explanation for withholding the document from destruction in the “Document Comment” property.

In cases where certain selected documents are routinely retained for a longer period than other documents in the record type, the longer retention value may be established in the file plan, which can permit the use of the file code to exclude the document from the global document status property change, and report of documents eligible for destruction. See the following discussion on the EDMS file plan.

**Reporting Records to be Destroyed**

Once the eligible records have been reviewed and approved for destruction, a report should be generated and attached to Form 1420, Records Destruction Log, for submission to Records Management. The report can make use of properties in the EDMS database and fields in the EDMS file plan, and should include the record type, record date, the retention code (Trigger Date and Years field from the EDMS file plan), and a reference to the agency item number on the records retention schedule (also in the file plan).

**Deleting the Records**

On completion of the report of records authorized for destruction, the EDMS system administrator may proceed with deletion of the records with the document status property “Delete.”

**Using the File Code Property**

When users select a record type and a document type when adding documents to the library, the selections associate the document with a file code—a unique numerical identifier that relates the document to a retention rule. The Excel EDMS File Plan spreadsheet also includes the retention trigger event, the number of years the retention is required, archival requirements (if any), and a citation to the TxDOT records retention schedule. System administrators can select fields from the
file plan for developing stored queries or scripts to accomplish operations on documents and collections of documents (records) in the library.

The file plan is posted on the EDMS intranet page and available via links from the ECM SharePoint site as well.

To employ the file plan, replace the “##” in the field(s) with your D/D/O’s functional account number (for example, “14” for the Austin district). Agency Item Number citations with a functional account number present refer to a division or office OPR for documents which may have a different retention requirement. In situations where a document exists in both district and division libraries, two separate entries in the file plan exist.

Assigning the functional account number relates the document contents to your specific D/D/O when citing the department’s records retention schedule in reports of records eligible for destruction or for attaching to Form 1420 upon completion of destruction. Multiple RRS Item references relate to records retention requirements for specific office operations. Records management can assist in selecting the appropriate reference for the particular library application being developed.

**Controlling EDMS Costs**

EDMS employs server-based technology which, in the current environment, represents a considerable cost to the department. While conscientious observance of file management/records retention and destruction procedures offers the possibility of establishing some equilibrium in storage requirements over time, the trend will be toward increasing storage needs as reference files of indefinite retention (“archival” files) are added.

Not all documents belong in an EDMS, and careful planning before implementing the technology can help to manage costs associated with the system. More detailed information on planning for EDMS is available in an [EDMS Planning Handbook](#).

Alternative approaches toward the management of archival files can reduce costs and improve security. Mass storage drives are inexpensive and can be duplicated with backups maintained in a separate location. Immediate online access is probably not that important for records stored in these devices, and the drives may be accessed “nearline” quickly enough for the majority of business processes that may need to call upon their contents.
Section 4 — Using a File Plan

Definition and Content

All TxDOT office or work units are required to develop and maintain a file plan. Records custodians must certify the currency and accuracy of their file plans to the DDO Records Administrator, who, in turn must certify the currency and accuracy of their organization's file plan to TxDOT Records Management.

The file plan discussed in this section is distinct from the EDMS file plan. A file plan is an index and a location guide to the information in files. It identifies record copy files to manage in accordance with the records retention schedule, retention requirements, and includes records being retained.

File plans must be reviewed and revised as necessary to maintain their utility for locating files. They can serve as a running inventory of an office’s records.

The standard department file plan is an Excel spread sheet that includes the following file plan information.

Table 4-1: File Plan Content

<table>
<thead>
<tr>
<th>Block</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Type</td>
<td>The record type may be a general description or a specific file name.</td>
</tr>
<tr>
<td>File Title/Description</td>
<td>File titles or descriptions identify major groups, minor groups and individual file folders. Major and minor group titles and descriptions may also appear on file guides in file cabinet drawers. Include instructions for standard electronic document/file naming conventions as applicable.</td>
</tr>
</tbody>
</table>
The following figure illustrates the file plan formats.

### Table 4-1: File Plan Content

<table>
<thead>
<tr>
<th>Block</th>
<th>Description</th>
</tr>
</thead>
</table>
| Location         | Files may be located in a variety of places. The file plan should guide users to the right place. For small offices, a general location statement may suffice. Larger offices may need to develop a numbering system for file cabinets and drawers or include a map or layout of the file cabinets with the file plan. File plans for electronic files may include directory paths and folder names, or by Document Class and Record Type properties in the EDMS. The following procedure is an easy way to copy and paste files in a shared drive:  
1. Open a blank worksheet in Excel with a wide column A.  
2. Open the shared drive and select List View.  
3. Highlight all folders.  
4. Right click and select Copy as Path.  
5. Paste to the first column and row in the spreadsheet. Note: The folders may not paste in the same order as originally displayed. Highlight the column and select Sort A to Z.  
6. Create enough rows in the file plan template to accept the folder list.  
7. Copy and paste the folder list to the file plan. |
| File Organization Description | Describe how files are organized. The description may include records and date range(s) in retention to be updated during annual currency review and certification.                                                                                                                                                  |
| Status           | Identify record copy files to help file management procedures related to retention and disposition of records.                                                                                                                                                                                                                                                   |
| Retention        | Enter retention periods for record copy files. Although information and convenience copies need to be retained only as long as needed, some offices include retention periods for them on the file plan if it is important to keep the records for specific periods.                                                                                                                                                                                                 |
| RSS Item         | For record copy files, the agency item number from the TxDOT records retention schedule is necessary when completing the records destruction log after purging files. Having it on the file plan is a convenient reference.                                                                                                                          |
Coordinating review and acceptance of the plan during its development among those who are responsible for and/or use the files helps to ensure filing accuracy. The file plan is a dynamic document that should be revised as needed.

## Certification

The Records Custodian shall certify the accuracy and currency of the file plan and forward a copy to the DDO Records Administrator. TxDOT Records Management sends an annual reminder to DDO Records Administrators to have their respective Records coordinators review and certify the currency and accuracy of their file plans. When local review is completed, the Records Administrator shall send an email to TxDOT Records Management certifying the currency and accuracy of the file plans within their organization.
Distributing the File Plan

Keep a copy of the file plan available at a central location for reference by employees. Making the plan available in an office’s shared drive or on an intranet site is an efficient method of dissemination. In hard-copy files, it may be helpful to insert a copy of the file plan at the front of each file drawer.

NOTE: It can also be helpful to maintain a file of previous file plans to use when records need to be retrieved from storage.

Support for Discovery and Open Records

DDO records administrators should maintain a file of current and recent file plans for their organizations to aid compliance efforts related to legal discovery and open records.
Section 5 — Hard Copy File Management

Visual Techniques

Section 1 discusses basic file organization principles and techniques. The principle of organizing for retrieval also applies to hard-copy filing systems.

Hard copy file management techniques include the use of file coding and folder labeling as primary retrieval aids.

File Coding

File coding is a shorthand identification of the major and minor group and folder number to identify where records are located and simplify routine filing and retrieval. File codes on folder labels and in file plans should mean something to users and help identify the contents of the file.

For example, a folder label has 3.CON 2 entered in the upper left corner. This file code represents the second file folder in the minor group Contracts (CON), in major group number 3, which may be business or project records that include contracts as a minor group. The label may also contain the contractor's name, the contract number or other identifying information.

The following table lists acronyms used in file codes of minor groups found in many offices. Create other codes as needed.

<table>
<thead>
<tr>
<th>Code</th>
<th>Minor Groups</th>
<th>Code</th>
<th>Minor Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC</td>
<td>Accounting, Stock Accounts, etc.</td>
<td>LIC</td>
<td>Licenses</td>
</tr>
<tr>
<td>ADM</td>
<td>Administrative Operations, Administration (may include accounting, budget, etc.)</td>
<td>LIT</td>
<td>Litigation</td>
</tr>
<tr>
<td>AGO</td>
<td>Attorney General's Office</td>
<td>MAN</td>
<td>Manuals</td>
</tr>
<tr>
<td>AGR</td>
<td>Agreements</td>
<td>MAP</td>
<td>Maps and charts</td>
</tr>
<tr>
<td>AUD</td>
<td>Audits</td>
<td>MAT</td>
<td>Materials Files, Materials Records</td>
</tr>
<tr>
<td>AUS</td>
<td>Austin Headquarters Correspondence, Reports, etc.</td>
<td>MGT</td>
<td>Management, Program Management, etc.</td>
</tr>
<tr>
<td>BRG</td>
<td>Bridge</td>
<td>MNT</td>
<td>Maintenance</td>
</tr>
<tr>
<td>BUD</td>
<td>Budget</td>
<td>PER</td>
<td>Personnel, Human Resources</td>
</tr>
<tr>
<td>CLM</td>
<td>Claims</td>
<td>PIO</td>
<td>Public Information, Public Relations</td>
</tr>
<tr>
<td>CON</td>
<td>Contracts, Contract Monitoring, etc.</td>
<td>PMT</td>
<td>Permits</td>
</tr>
</tbody>
</table>
Organizing and Labeling File Folders and Guides

Each file folder holds a specific set of related records. There are a number of ways to arrange file folders within a major or minor group. Keep the following in mind when organizing files:

- Think about retrieving information rather than storing paper.
- Use specific titles for major groups, minor groups and file folders, leaving no room for misinterpretation. Do not use "Miscellaneous" as a title; it is another word for "lost."
- Arrange folders functionally and logically. The arrangement should relate directly to office functions and provide the most convenient access to the most active files.
- Use color to distinguish files that are purged routinely from files retained for a long time. Colored labels may identify a specific time period, such as calendar or fiscal year. The less that retention periods vary among various folders, the easier it is to manage the files. White labels can identify files that are not routinely purged.

<table>
<thead>
<tr>
<th>Code</th>
<th>Minor Groups</th>
<th>Code</th>
<th>Minor Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>COR</td>
<td>Correspondence</td>
<td>POL</td>
<td>Policies</td>
</tr>
<tr>
<td>CUR</td>
<td>Current Directives, Current Project, etc.</td>
<td>PRE</td>
<td>Preliminary Bids, Preliminary Plans, etc.</td>
</tr>
<tr>
<td>DD</td>
<td>Division Director (or OD for Office Director)</td>
<td>PRG</td>
<td>Program Files (or files related to ongoing functional programs, etc.)</td>
</tr>
<tr>
<td>DE</td>
<td>District Engineer</td>
<td>PRO</td>
<td>Project Files, Procedures</td>
</tr>
<tr>
<td>DIR</td>
<td>TxDOT Directives, Administrative Circulars, Administrative or District/Division Announcements, etc.</td>
<td>PUB</td>
<td>Publications, Public Hearings</td>
</tr>
<tr>
<td>EEO</td>
<td>Equal Employment Opportunity</td>
<td>PUR</td>
<td>Purchases, Purchase Orders</td>
</tr>
<tr>
<td>EQP</td>
<td>Equipment (use MAJ or MIN if needed)</td>
<td>REF</td>
<td>Reference</td>
</tr>
<tr>
<td>FIN</td>
<td>Financial</td>
<td>REG</td>
<td>Regulations</td>
</tr>
<tr>
<td>GEN</td>
<td>General Correspondence, General Reports, etc.</td>
<td>REQ</td>
<td>Requirements, Requisitions, Requests</td>
</tr>
<tr>
<td>INR</td>
<td>Internal Reviews, Internal Audits, Sunset</td>
<td>RES</td>
<td>Resident, Research</td>
</tr>
<tr>
<td>IPE</td>
<td>Investigation and Planning Expense</td>
<td>RPT</td>
<td>Reports</td>
</tr>
<tr>
<td>ISS</td>
<td>Issues</td>
<td>RRX</td>
<td>Railroad Crossing</td>
</tr>
<tr>
<td>LED</td>
<td>Ledgers</td>
<td>SAF</td>
<td>Safety</td>
</tr>
<tr>
<td>LEG</td>
<td>Legal, Legislative, Legislature</td>
<td>TOR</td>
<td>Tort Claims</td>
</tr>
<tr>
<td>LET</td>
<td>Letting Files, Letters</td>
<td>TRN</td>
<td>Transitory Files, Reading Files</td>
</tr>
</tbody>
</table>

Table 4-2: Minor Groups and Codes
Include reference to automated or non-standard records and files. Use file guides to tell users that automated or imaged files exist, where they are and how to access them.

Setting Up Files

Steps in organizing hard copy files include
- preparing file guides,
- preparing labels for file folders and drawers,
- coding records,
- cross-referencing files,
- organizing files according to the file plan, and
- distributing the file plan.

Preparing File Guides

Prepare a file guide (divider) for each major and minor group of file folders.

Major group guides should include the major group number and title, “1. ORGANIZATION AND MANAGEMENT,” for example minor group guides should include the appropriate major group number, minor group code, and minor group title. For a minor group of audit folders within the major group of organization and management, the guide label would consist of “1. AUD Audits.”

Major group guides should be distinguishable from minor group guides at a glance. An easy way to do this is to use a second-position guide (center tab) for major groups and a first-or third-position guide (tab on the left or right) for minor groups.

NOTE: For electronic files, microfilm files or files located away from the file cabinets, prepare a guide that tells where to find the files. For example, if files are maintained electronically on a shared drive, a directory address, such as “SEE T:\Folder\Sub-folder name” may be useful.

When using color coded folder labels as a file management tool, use plain white guide labels to avoid having to prepare new file guides every year.

Preparing Folder Labels

Use color-coded labels to distinguish folders maintained on a periodic (fiscal or calendar year) basis, and white for folders that are not routinely purged which remain in the files year after year.
The folder label describes where a folder belongs in the files and what is in it. Each label should include the file code, folder title or content description and, if needed, a date for the contents.

Although space on labels is limited, including additional information, such as identification of record copies and destruction date can be helpful in file management.

For extensive or complicated filing systems, labeling systems using large, easily visible letters, numbers and dates in varying color combinations and tab configurations are available from commercial vendors. Bar code technology is also commercially available for large file systems with significant retrieval activity.

**Preparing File Drawer Labels**

Use file drawer labels to identify the contents of each drawer. If room permits, list the titles and/or codes, dates or other identifying information for beginning and ending major and minor groups in the drawer.

**Coding Records for Filing**

Ease of retrieval and successful file management depends on accurate filing. Entering the file code on a document tells at a glance where it belongs in the files. The most effective method of coding is to enter the appropriate file code, consisting of the major group number, three-letter minor group acronym, and appropriate folder number in a prominent place, such as the upper right corner on each document as a routine office procedure when documents are created or received. This can be automated somewhat by including the file code in headers or footers on template documents related to particular functions or activities. It may not be feasible to code all existing files, but when a file is retrieved, it can be coded for accurate refiling.

Documents copied and filed in different locations need more than one code. Circle the code for the file folder where the particular copy of the document belongs.

**Cross-References**

Avoid filing multiple copies of records. When a record appears to belong in more than one place, prepare a file guide pointing to the proper location of the record. This method reduces the chance of inadvertently retaining convenience copies after the record copy has been destroyed.

An alternative is to use the "Remarks" area on the file plan to cross-reference files.
Charge-Out Records

When a user removes a file folder from the files, the folder should be replaced with a charge-out record card containing the date of removal, a brief description of the folder removed (label information usually suffices), and the name and phone number of the user.

Standard charge-out record cards (Form 1418, Charge-Out Record -- DHT# 122641) are available from TxDOT supply sources. It is a good idea to keep a few cards at the front of each file drawer. When a user returns a checked out folder, the user's name can be marked out and the card re-used.

Problems in File Organization

Basic organization moves from the broad functional area to subdivisions of the area to the specific files. The most common problems in organizing files are:

Too many major groups with only one or two minor groups in each result in a complex and confusing filing system. Limiting the major groups to the broadest categories of major functions or areas of activity for the office helps reduce major groups to a manageable number.

Too many minor groups with only one or two folders in each, result in too many sub-categories to remember and can increase the chance of misfiles. Major groups may have a number of minor groups. Carefully determining the scope of major groups will help you control the number of minor groups. A simple and balanced system reduces misfiles and lost records. It costs approximately $100 each time a file is misplaced in a large office.
Section 6 — Conducting Routine File Closing Procedures

Benefits

Conducting routine file closing procedures reduces clutter in files, enabling more efficient retrieval. The procedures also reinforce consistent compliance with records retention requirements by helping employees become comfortable with moving records to storage and ultimately destruction as a routine business procedure.

Establishing a Routine

File closing consists of declaring a file a record for retention purposes and arranging for its secure retention. Typical triggers for record declaration are the completion of a project or process or calendar-based operations occurring at the turn of the fiscal or calendar year.

For documents or records stored as scanned images or retained in their native application in an EDMS, it is generally more efficient to integrate scanning or addition to the FileNet repository at the point the record would ordinarily be filed rather than waiting to perform batch scanning operations.

While regularly conducting closing procedures as file processes are completed offers certain efficiencies, offices may better coordinate procedures using a calendar-based routine that provides checks to ensure declaration and capture of electronic records for retention or destruction.

Coordinating Procedures

Closing hard copy files and arranging storage for retention is a straightforward process. Managing the procedures in a mixed or entirely electronic format, however, requires additional steps to ensure a coordinated process:

- Include migration from individual desktops to the shared drive for records/documents maintained on shared drives.
- Coordinate the deletion of copies from desktop workstations.
- Unless required for retention, delete working files or drafts from shared drives and delete inactive SharePoint sites after taking steps to preserve any content from the sites that may require retention.
- Include addition of completed documents to the FileNet repository.
- Request global document property changes/uploads as appropriate for record documents in the FileNet repository. These may include document or process status, date and comment properties.
Purging Procedures

Review files at least annually to remove inactive records for storage or to destroy eligible records. Since most TxDOT records are filed and retained on a fiscal year basis, purging can be undertaken while new files are being set up for the next fiscal year. Purge transitory, convenience or information files more often, if needed. The file plan can be a helpful tool, if it identifies record copy files and includes retention periods.

Table 4-3: File Purging Procedures

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Print out a copy of the file plan to mark up indicating files to be stored and files eligible for destruction.</td>
</tr>
<tr>
<td>2</td>
<td>Make a list of the records to be stored in sufficient detail for efficient retrieval. Form 1419, “Records Transfer and Service Request” is a document designed for that purpose. An index of files being purged for immediate destruction may be more general, but should contain sufficient information to identify the records being destroyed to enter on Form 1420 Records Destruction Log, if they are record copies.</td>
</tr>
<tr>
<td>3</td>
<td>Identify any records with a State Archives review requirement on the records retention schedule and mark them for coordination with Records Management at the end of their retention period.</td>
</tr>
<tr>
<td>4-a</td>
<td>Remove files to be stored at a different location and place them in an appropriate container, such as the standard document box (NIGP # 615-37-13-0850) available from department supply sources. Since most required retention periods are relatively brief, it may be convenient simply to designate unused file cabinets or drawers as storage areas for documents being retained.</td>
</tr>
<tr>
<td>4-b</td>
<td>Coordinate a review of files on desktops to ensure migration to an appropriate location on either a shared drive or EDMS. The review should include deletion of drafts, notes, or working copies, as appropriate. Records kept only in electronic format may be moved to off-line storage media or special folders set up for storage. See Chapter 5, Electronic Records for specific information and requirements related to retention of electronic records.</td>
</tr>
<tr>
<td>4-c</td>
<td>Delete any inactive SharePoint sites after saving any content requiring retention as a record.</td>
</tr>
<tr>
<td>4-d</td>
<td>Custodians of records in an electronic document management system (EDMS) can change the status property to declare documents or collections of related documents as records for retention purposes. A search based on a combination of properties, such as record type, date, and status can identify documents meeting the criteria that designate them as records. Custodians and systems administrators can use the file code property to initiate global actions to revise any status properties to “Final” or “Complete” to declare the documents as records and to initiate their retention.</td>
</tr>
<tr>
<td>5</td>
<td>Coordinate a review of records eligible for destruction with the appropriate manager, supervisor, custodian and/or records coordinator responsible for the records to authorize destruction on the records destruction log or identify any records that must be withheld from destruction*. Refer to Chapter 10, Records Destruction, for detailed records destruction procedures.</td>
</tr>
</tbody>
</table>

* Records involved in an audit, investigation, litigation hold or public information request will typically have been retrieved or otherwise identified. If there is a reasonable anticipation of legal action involving any particular records, check with OCC and OGC before authorizing their destruction.
Chapter 5 — Electronic Records

Contents:

Section 1 — Definition and Overview
Section 2 — Requirements for Managing Electronic Records
Section 3 — General Practices for Managing Electronic Records
Section 4 — Managing Email Records
Section 5 — Records Management in an EDMS
Section 6 — Risk Management and Electronic Records
Section 1 — Definition and Overview

Definition of Electronic Record

An electronic record is any information created, used and retained in a form that only a computer can process. Electronic records include email, text messages, disaster recovery backup tape, and records that exist on portable media, such as memory sticks, BlackBerry devices, or PDAs. Records related to department work that may be produced or kept on personal devices away from the office are considered state records, and are not the employee's personal property.

Any state record may be created or stored electronically. Certified output from electronically digitized images or other electronic data compilations is accepted as original state records by any court or administrative agency of this state unless barred by a federal law, regulation, or rule of court.

The definition of a record can range from a single document to entire files of different types of applications and media related to the conduct of official business. In this chapter, the term record and file may be used interchangeably to describe official records, as distinguished from the use of these terms to describe specific data sets in the computing environment.

Chapter Overview

This chapter

◆ defines electronic records,
◆ summarizes requirements for managing electronic records,
◆ discusses practical procedures and best practices for managing electronic records during the inactive portion of their life cycle,
◆ discusses management of email records,
◆ discusses records management planning in the development of electronic document management systems, and
◆ discusses risk management and electronic records.
Section 2 — Requirements for Managing Electronic Records

Introduction

Records management principles and requirements apply to official records that are created and maintained in any medium. 13 TAC §6, Standards and Procedures for the Management of Electronic Records, establishes requirements related to the creation, retention and disposition of electronic state records.

The rules require that state agencies establish procedures for the management of electronic records that ensure

- software, hardware, and documentation for retrieving records are retained throughout the retention period of the records or that records are migrated to another system;
- necessary maintenance is performed to ensure that records are preserved;
- records are identified as part of a records series and that they are individually accessible;
- email systems preserve essential basic metadata and email is appropriately retained;
- destruction of records protects the confidentiality of confidential and sensitive records;
- records are destroyed in compliance with an approved records retention schedule.

The rules also require that agencies

- provide a training program for users in the operation, care, and handling of the information, equipment, software, and media;
- maintain current documentation that is adequate for retaining, reading, and processing the records; and
- administer a security program in compliance with 1 TAC §202.

Chapter 4, File Management, discusses organization and management of electronic files in support of active business processes. This chapter focuses on procedures and best practices for the management of inactive electronic records during their required retention period.
Section 3 — General Practices for Managing Electronic Records

Working Files and Record Copies

Electronic working files such as raw data, drafts, working copies, etc. ordinarily only need to be retained until their purpose is served or they are updated. Any resulting official record to be kept electronically is to be retained for the required period in a secure manner that prevents alteration of the record. If an electronic draft or working copy of a record remains in a records system or on a disk after the destruction of the final version or "official" record, the electronic draft or working copy becomes the record copy.

Retaining Electronic Records

Chapter 4 discusses procedures for managing files in all media. The FileNet enterprise document management system (EDMS) is the preferred medium for retaining electronic records created in MS Office applications and email. In some cases local shared drives may be used to retain electronic records for their required retention period, but the EDMS offers better security to maintain document integrity after declaration of a record, and assures the actual destruction of the electronic record after its retention period has been met. Memory capacity is a consideration in planning for the retention of electronic records. Electronic forms and documents containing macros consume significant amounts of memory.

Avoid using individual desktop workstations to retain official records, as the practice exposes records to potential loss when employees leave or when equipment and software is upgraded.

Include electronic records management procedures in written office operating procedures.

Using Offline Media

Portable offline media such as CDs, tapes or diskettes should only be used to retain records that have a short retention requirement, as equipment or software replacements may render the media obsolete or unusable. Individual offline media should contain only a single record series or closely related record series that have the same destruction date. Records must be individually accessible. Do not use routine backup media for record keeping purposes. Records being retained on diskettes or other portable media for retention are to be kept on media dedicated to that purpose only.

Electronic storage media must have an external label or an index that includes:

- name or other identifier of the organizational unit responsible for the records;
- descriptive title of the contents;
- dates of creation and authorized disposition date;
Maintaining Offline Media

Offices retaining electronic records must establish a schedule for recopying electronic state records maintained on electronic media to ensure that no information is lost.

- Recopy records maintained on floppy disks (diskettes) a minimum of once a year.
- Records on more durable media should be inspected and recopied on a regular interval if they are retained for more than five years or if the media is frequently used to access the records. Most department records have a retention period shorter than five years.
- Offices maintaining electronic records on offline media must have a migration strategy in place to ensure the availability and usability of the electronic record across hardware and software changes until the expiration of its retention period.
- Keep electronic media away from sources of electromagnetic radiation such as magnets and motors.
- Protect diskettes. Keep diskettes in a clean space with dust protection and out of direct sunlight. Avoid touching the surface of diskettes or other storage media; skin oils can interfere with their ability to store data.
- Maintain proper temperature and humidity. For records retained less than 10 years, an air-conditioned office environment usually suffices. Ideally, diskettes and cassettes should be kept in 65°F to 75°F temperature and 30% to 50% relative humidity. Optical data storage media are more environmentally tolerant, requiring 14°F to 122°F temperature and 10% to 90% relative humidity.

13TAC§6.96 describes specific standards and procedures related to the maintenance of storage media in data tape libraries and storage facilities, and standards for optical media used to store electronic records as digital images. Department offices retaining records in this manner can access the requirements by clicking on the hyperlink.

Protecting Record Integrity

It is essential to ensure that records are not changed, damaged or destroyed before their retention period is over. Extra care is necessary when relying on an electronic record keeping system. Electronic records must be maintained in a usable format until their authorized disposal date, and must be secured from inadvertent alteration or deletion. Security procedures may include identifying custodial responsibility for specific records retained electronically, and using security features to
limit access to the records during their retention to the designated custodian only. In an EDMS, restricting the rights to documents to Read-Only can contribute to the integrity of the record. The procedure should include a method of logging any access or retrieval of the record during its retention.

**Securing Confidential Records**

Every employee is responsible for exercising appropriate care for official records. The policies and procedures described in Chapter 10 of the online Information Security Manual apply also to sensitive or confidential records that are retained electronically.

Security measures for retaining confidential electronic records include:

- Add the record to the EDMS with document access rights restricted to the minimum number of employees/users required for the record.
- Create the original record on a diskette so that the information is not part of any directory on a hard drive.
- Copy them to offline media, which can be physically secured under lock and key, with access limited to authorized persons.
- If retaining confidential records on a PC or server is unavoidable, limit access to the records by the use of additional password or operating system security.
- Remember that, except for the EDMS, deleted records remain on the hard drive even though they are not shown on the file directory. Consult with your information resources administrator to ensure the removal of the record from the disk itself and any backup media after it has been copied to offline media or otherwise deleted.

The only sure way to destroy confidential files on portable storage media is to physically destroy the media.

**Document Imaging**

Base the decision to convert documents or records to digital images on an actual business need. Keeping records “just in case” a legal need may arise is not a legitimate business need. The costs to scan hard-copy originals simply for retention purposes are not usually justified in comparison to the lower cost simply to box and store records that have a relatively short retention period and that are not subject to frequent retrievals.

Imaging is a good solution for retaining records that are subject to frequent retrieval during their retention. Imaging also offers savings in space and filing equipment for voluminous records, and can be useful for maintaining duplicate copies of records as part of a vital records protection program. Maintenance of image files incurs costs for server space, however.
Selection of the image file format is a consideration. Adobe Acrobat’s PDF offers some functionality in imaged documents, and, since the reader has been made freely available, PDF has become a de facto standard. If the requirement for an imaged record is simply to retain it without a need for any added functionality, use of the Tagged Image File Format (TIFF), a graphic file format developed by Aldus and Microsoft, is sufficient and usable by standard image viewers.

Length of retention of the imaged records is also a consideration. Changes in technology do not generally represent a threat to the ability to access and read records being retained on a particular electronic medium for fewer than five years. Migration strategies and the budgeting necessary to implement them are an important consideration in any planning for long-term retention of records on electronic or digital media.

In most cases it is best to implement scanning from a point forward. Backfile conversion (scanning of files currently in storage) is normally not cost-effective.

Integrating scanning procedures into the workflow can address both active file retrieval and record storage needs while avoiding the added separate step in the handling of records that batch processes involve. For example, scanning files when they would normally be closed and filed can spread the workload over time. The scanned images can reside in memory until it is time to create the CD for retention.

Imaging should be documented as a routine business practice in written and dated internal office procedures. Include information on when in the record or document's life it is scanned, quality control measures employed, disposition of the original record or document, retention of the imaged records, procedures for authorization and destruction of the CD. Click here to access an example of a scanning procedure document in use in a headquarters division.

Requirements and Recommendations for Imaged Records

The following information only includes standards and processes that must be followed for compliance with state statutes and rules, as well as recommended accepted industry standards. The owner of the system needs to document specific internal procedures and training manuals. Also, there are additional requirements that are not included in the above, if the scanning project incorporates any of the following:

- Optical Character Recognition (OCR)
- Intelligent Character Recognition (ICR)
- Web-Based Document Management Technology
- Electronic Transactions and/or Electronic Signatures
**Requirements:** The rules in 13 TAC §6.91-6.97 require that the following standards must be met for electronic records stored as digital images:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Action</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>A non-proprietary image file header label must be used.</td>
<td>If a proprietary image file header label is used, a bridge to a non-proprietary image file header label or a detailed definition of image file header label structure must be provided.</td>
<td>13 TAC §6.96 (f) (1)</td>
</tr>
<tr>
<td>System hardware and/or software must provide a quality assurance capability that verifies information written to the storage media.</td>
<td>Provide written instruction and training for staff to use to verify.</td>
<td>13 TAC §6.96 (f) (2)</td>
</tr>
<tr>
<td>Scanned image quality must be evaluated according to the standard procedures in ANSI/AIIM MS44*.</td>
<td>Detailed the in the table below for ANSI/AIIM MS44-1988 (R1993) standard.</td>
<td>13 TAC §6.96 (f) (3)</td>
</tr>
<tr>
<td>A visual quality control evaluation must be performed for each scanned image and related index data.</td>
<td>Detailed the in the table below for ANSI/AIIM MS44-1988 (R1993) standard.</td>
<td>13 TAC §6.96 (f) (4)</td>
</tr>
<tr>
<td>A scanning resolution with a minimum of 200 dots per inch is required for recording documents that contain no type font smaller than 6 point. For documents with a type font smaller than 6 point, scanning resolution must be adequate to ensure that no information is lost.</td>
<td>Detailed the in the table below for ANSI/AIIM MS44-1988 (R1993) standard.</td>
<td>13 TAC §6.96 (f) (5-6)</td>
</tr>
<tr>
<td>The selected scanning resolution must be validated with tests on actual documents.</td>
<td>Detailed the in the table below for ANSI/AIIM MS44-1988 (R1993) standard.</td>
<td>13 TAC §6.96 (f) (7)</td>
</tr>
<tr>
<td>The use of the International Telecommunication Union-Technical (ITU-T) Group 3 or Group 4 compression techniques is required for document images without continuous tonal qualities.</td>
<td>If use of a proprietary compression technique is unavoidable, a gateway to either Group 3 or Group 4 compression techniques must be provided.</td>
<td>13 TAC §6.96 (f) (8)</td>
</tr>
</tbody>
</table>

* American National Standard for Information and Image Management—Recommended Practice for Quality Control of Image Scanners (most current version of ANSI/AIIM MS44).
**Recommended industry practices:** The following table lists requirements from ANSI/AIIM MS44-1988 (R1993) - Standard for Information and Image Management - Recommended Practice for Quality Control of Image Scanners:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Action</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use standard original targets</td>
<td><strong>Purchase targets</strong> from AIIM. Do NOT use copies of targets!</td>
<td>ANSI/AIIM MS44-1988 (R1993) 7. Target 1: IEEE</td>
</tr>
<tr>
<td></td>
<td>A photocopy of <strong>Target 1</strong> will render it useless for determining at what level of grey the scanner decides a point is black.</td>
<td>8. Target 2: AIIM Scanner Target</td>
</tr>
<tr>
<td></td>
<td>A photocopy of <strong>Target 2</strong> will destroy the usefulness of size, placement, black, and halftone test areas.</td>
<td></td>
</tr>
<tr>
<td>Determine number of document types</td>
<td>Inventory documents to determine how many <strong>different types of documents</strong> to be scanned. Consider different sizes, colors, amount of white space, etc.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 4.3 Establishing a Quality Reference</td>
</tr>
<tr>
<td>Establish a quality reference for “good output” for each type of document</td>
<td>Scan all targets, output to hardcopy, and examine. Keep hardcopy and store digital images. <strong>Note scanner adjustment</strong> on settings on the hardcopy.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 4.3 Establishing a Quality Reference</td>
</tr>
<tr>
<td>Determine when to change scanner settings</td>
<td>Batch documents; change scanner settings for batch; or (2) Change scanner settings for each document scanned.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 5. Frequency of Testing</td>
</tr>
<tr>
<td>Testing for batch documents</td>
<td>Perform a <strong>test run before and after scanning</strong>. Results should be the same for both.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 4.3 Establishing a Quality Reference</td>
</tr>
<tr>
<td>Testing after each scanned document</td>
<td>Determine a small number of <strong>allowable settings</strong> for each document type.</td>
<td>ANSI/AIIM MS44-R1993 4.3 Establishing a Quality Reference</td>
</tr>
<tr>
<td>Test after maintenance</td>
<td>After <strong>recalibration</strong> by a technician, perform a <strong>test run</strong> of all targets.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 4.3 Establishing a Quality Reference</td>
</tr>
<tr>
<td>Recordkeeping</td>
<td>Each <strong>test run</strong> should be <strong>recorded</strong> on a log sheet. Log can spot a problem earlier; ex: threshold setting keeps changing in one direction. If it is an equipment problem, note scanner settings on the back of the printout and save for technician.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 4.5 Record Keeping</td>
</tr>
<tr>
<td>Frequency of test runs</td>
<td>Perform <strong>test run</strong> before and after each batch is scanned. No limit to batch size, but frequent testing recommended. Terminate each batch at end of a shift.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 5. Frequency of Testing</td>
</tr>
<tr>
<td>Requirement</td>
<td>Action</td>
<td>Source</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set up scanner parameters</td>
<td>Set up parameters to match original scan parameters or the most recent quality reference.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 6.1 Setup of Scanner Parameters</td>
</tr>
<tr>
<td>Placement of targets</td>
<td>Place targets on scanner in same manner as original documents will be processed.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 6.2 Placement of Target on the Scanner</td>
</tr>
<tr>
<td>Scanning</td>
<td>Scan targets using same procedures for original documents. Do not change settings between targets. After printed image is evaluated, electronic test images may be erased or stored.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 6.3 Scanning</td>
</tr>
<tr>
<td>Examine targets on screen</td>
<td>Test targets may be viewed on screen until a good test run is achieved; however, there is no easy way to compare a current scan against reference scan. Also, display may not show full page. Easier to compare paper.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 6.4 Examination of Targets on Screen</td>
</tr>
<tr>
<td>Printing targets</td>
<td>Test scans should be output to paper. Provides end-to-end system check. Can quickly determine if output is acceptable.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 6.5 Printing of Targets</td>
</tr>
<tr>
<td>Determination of problem areas</td>
<td>If printed output is not acceptable, check printer by retrieving a quality reference and printing. If output is not acceptable, it is probably a printer problem. If output is acceptable, it is probably a scanner problem.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 6.6 Determination of Problem Areas</td>
</tr>
<tr>
<td>Target 1: IEEE Std 167-A1987 (Institute of Electrical and Electronics Engineers)</td>
<td>This target is a facsimile machine test target, which provides a continuous-tone photograph, gray scale, precision measurement marks, resolution charts, and test characters.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 7. Target 1: IEEE</td>
</tr>
<tr>
<td>Target 1 (continued)</td>
<td>Grey scale shows the threshold point at which the scanner decides that a given area is black rather than white. Run the target and observe the point at which the bars turn from white to black. The continuous wedge will have ragged appearance at transition area. In daily testing, observe if the white-to-black transition points are in the same place as on reference copy. If so, threshold setting is properly adjusted. Use Patterns #7 and #8 on the target to test grey scale.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 7.1 Threshold for Grey Levels</td>
</tr>
<tr>
<td>Requirement</td>
<td>Action</td>
<td>Source</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Target 1 (continued)</td>
<td>(2) <strong>Resolution</strong> is a measurement of the output quality of an <strong>image</strong>, usually in terms of samples, pixels, dots, or lines per inch. At the center the lines are very narrow and will blur at varying distances from the center. The distance of the blurring from the center is an indication of the resolution of the total system. Use <strong>Patterns #12 and #13</strong> to test scanner resolution.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 7.2 Resolution</td>
</tr>
<tr>
<td>Target 1 (continued)</td>
<td>(3) <strong>Linearity</strong> and <strong>Rectangularity</strong> involves testing the calibration to make sure that the system is not distorting images. The <strong>length</strong> of line on the copy should match the length of lines on the original. All lines should be straight, and lines on opposite sides should be equal. The <strong>rectangularity</strong> of the image is perfect if the length of opposite sides are equal and the distances between the diagonal corners are identical.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 7.3 Linearity and Rectangularity</td>
</tr>
<tr>
<td>Target 1 (continued)</td>
<td>(4) The <strong>text</strong> can be tested by examining the smallest legible type. This should not vary between the daily test runs and the quality reference. Though explained under Target 1, it recommends the use <strong>Target 2</strong> for this test.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 7.4 Text</td>
</tr>
<tr>
<td>Target 2: AIIM Scanner Target</td>
<td>This target is an ink-on-paper target that <strong>simulates conditions</strong> that may cause <strong>scanner problems</strong>.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8. Target 2: AIIM Scanner Target</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>Check to ensure that the <strong>scan area is the proper size</strong>. If the black boxes in the corners of the target do not run off the edges of the scanned image, the scan area may be too large. If the “0” digit in the line of numbers at the corners of each page are not visible on the scanned image, the scan area is too small, or the target was not properly aligned. Note: Some printers do not print to the edge of the paper – this should be taken into consideration.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.1 Size of Scan Area</td>
</tr>
<tr>
<td>Requirement</td>
<td>Action</td>
<td>Source</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(2) Check the <strong>alignment of the page</strong>. If the scan area is the proper size and target is perfectly aligned, the “0” digit will show at all corner and at the center of each edge. If the image size or printout size is reduced, look for the same numbers appearing at all points.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.2 Alignment of Page</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(3) Check the <strong>text</strong> by examining the small characters and punctuation to determine where scanning problems may occur. Look for legibility and detail of the small characters, such as the serifs on small characters. Examine the News Gothic Bold Reverse font for character lines that may be filled with black. It is important to know at what type size the scanner will lose the distinction between lower case letters such as a, e, c, and o. A properly adjusted scanner with 300 dots per inch should preserve these characters in a 4 point type.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.3 Text</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(4) There should be <strong>five horizontal and five vertical lines</strong> on the page. Verify that the thinnest line is visible. Note that stair-stepping in the lines is normal if the target is not exactly parallel to the scan lines.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.4 Horizontal and Vertical Lines</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(5) The <strong>diagonal line</strong> across the target is a test for uniform transport movement. The line should be smooth and straight within the capability of the scanner and recorder. Breaks in the line may indicate that a mechanical transport is not working smoothly, or is being forced to pause and restart.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.5 Diagonal Line</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(6) The <strong>isolated characters</strong> simulate a page number or part of a mathematical equation. Because of the large white space around each character, some scanners will see these characters as dirt specks and eliminate them. Some scanners will fail on the degree symbol (last column, center row) and display it as a solid dot.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.6 Isolated Characters</td>
</tr>
<tr>
<td>Requirement</td>
<td>Action</td>
<td>Source</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(7) The <strong>black-and-white areas</strong> allow solid areas for density checking using a densitometer. Normally, visual examination is sufficient to determine if the white area is clear and the black area is solid black. Failure to show the black area as solid black is usually a printer problem rather than a scanner problem, and the printer should be checked using the reference image. <strong>NOTE:</strong> Densitometric values for images that are output using toning processes vary significantly from the silver halide-based systems. Be aware that measurement of toned images could be unique to that system. There is no standard for comparison of these measurements.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.7 Black-and-white Areas</td>
</tr>
<tr>
<td>Target 2 (continued)</td>
<td>(8) <strong>Halftones</strong> pose a problem for most scanners because there are only a small number of scan lines across each half-tone dot. This results in a moiré pattern, which will vary according to the scan resolution, halftone mesh (dots per inch), angle of the target, and placement of the target. The only way to eliminate moiré is to scan at high resolutions (more than 1,000 lines per inch). The <strong>evaluation criteria</strong> are the lightest (smallest) halftone dot that the scanner will recognize and the darkest (largest) halftone dot area that the scanner will not see as solid black. The halftone mesh (halftone dots per inch measuring along a 45 degree angle) should be 85 to 110 mesh. During a normal test run, examine the lightest box visible and the darkest box that is not solid black for each halftone mesh. These should be the same as on the quality reference output. The threshold setting of the scanner will have a direct effect on this test.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 8.8 Halftones</td>
</tr>
<tr>
<td>Target 3: RIT Process Ink Gamut Chart</td>
<td>This target is a chart representing the <strong>range of colors</strong> that can be printed using standard process inks. If scanning involves using a color printer, there is additional information in the standard that is not included with this information.</td>
<td>ANSI/AIIM MS44-1988 (R1993) 9. Target 3: RIT Process Ink Gamut Chart</td>
</tr>
</tbody>
</table>
**Destruction of Electronic Records**

The procedures for destroying electronic records at the end of their retention periods are the same as for other records, and require proper documentation of destruction. See Chapter 10, “Records Destruction Log.”

Destroy convenience or information copies, working drafts and other non-record copies when they have served their purpose.

Deletion of electronic records simply removes the index pointer to the document/folder, and does not destroy them. Over time and with continued use of the disk they will become fragmented and virtually inaccessible, but will nevertheless remain forensically reconstructible. For most records, deletion is satisfactory for "destruction" purposes. For sensitive or confidential records, physical destruction or reformatting of the medium is necessary to assure proper destruction of the record.

Documents deleted from the FileNet EDMS are truly deleted and are unrecoverable.

Destruction of electronic records should be coordinated with procedures to assure their simultaneous removal from backup media.

Electronic records having archival value must be maintained by the agency except as otherwise determined by the state archivist. Electronic records must be retained with the hardware and software appropriate to retrieve and read the record. Offices choosing to retain archival state records electronically must establish a migration strategy to ensure that the records are retrievable and readable with whatever technology is currently in use in the department. An alternative is to print the records out on acid-free paper, and to contact records management to coordinate their handling with the state archivist.
Section 4 — Managing Email Records

Managing Email Records


Email messages created or received using TxDOT resources and/or in the course of TxDOT business are considered state records and are subject to the same requirements that relate to all official state records. Most email records have a short-term value, but the content may be such that the email is subject to retention in accordance with the requirements for a particular record series in the TxDOT records retention schedule.

Because of volume, email presents a potentially expensive liability in terms of discovery or open records requests. See the subheading, "Email Best Practices" in Section 6, "Risk Management and Electronic Records," for guidelines to reduce negative exposure in email records.

It is inappropriate to use email systems to store email that must meet retention requirements, since storage capacities for email systems and servers vary, and since email folders and archiving tools are routinely eliminated when employees depart.

In the absence of technology-based enterprise email and electronic records management applications, management of email records must begin with basic techniques that include organization of the records, employee training, and establishment of routine management procedures. Reliance on manual methods of email management is the least desirable approach, but lack of technological solutions should not deter efforts to responsibly manage these records. The following techniques, detailed in the remainder of this section, address managing and retaining email messages using resources that are currently available to managers and supervisors:

- email classifications
- employee training
- content templates and naming conventions
- email retention

Classifying Email

It is estimated that only about 10 to 15 percent of a typical organization's email is business-related. The first step in managing email is classifying messages in one of three categories: transitory, operational or executive (administrative).

- Transitory email messages have content of temporary usefulness and do not need to be regularly filed in a record keeping system. Transitory messages may be needed for a limited period of time for the completion of a task or action. Examples include routine messages that do not
fulfill statutory obligations or document specific agency (business) transactions or functions, such as meeting notices or transmittals that add nothing of value to attachments.

- **Transaction-related** email messages, such as memos or reports, relate to specific business functions or transactions and must be filed with the appropriate record series. The content or properties of this email document fulfillment of statutory obligations or routine agency transaction or functions.

- **Executive or Administrative** email messages are typically subject to State Archives review requirements, and include communications at executive or program administration levels of the agency operations that document
  - fulfillment of statutory obligations,
  - policy or procedural development or implementation, and/or
  - program administration transactions or functions, including formulation, planning, implementation, interpretation, modification or redefinition of programs, and services or projects and the administrative regulations, policies and procedures that govern them.

**Employee Training**

Managers and supervisors should specify which email records in everyday operations require retention, and train employees in routine procedures to capture the records.

**Content Templates and Naming Conventions**

Use of templates and subject naming conventions help control content, make classification more intuitive, and make individual emails more accessible for retrieval.

Establishing standardized text for naming routine communications related to business functions can help eliminate inconsistencies and informalities that may suggest impropriety. Standard templates with "fill in the blank" capabilities can be developed in MS Word and maintained on a shared drive for use by employees for internal and external business transactions or for public communications. Templates should be developed and approved by appropriate levels of management and, when necessary, reviewed by OGC before implementation.

Naming conventions for content in a message's subject line facilitate identification and retrieval of email. Naming conventions should focus on functions and use a combination of keywords and identification criteria such as case, CSJ or PO number.

**Capturing Email for Retention**

Best practices in email management include maintaining email in a central repository. Offices may employ a local shared drive as a repository or, preferably, the FileNet EDMS.
Shared drive repositories should include a folder structure designed for email retention, as described in Chapter 4. Using document naming conventions for content in subject lines can facilitate future identification for email messages saved as documents.

EDMS repositories are preferred for retention. When adding documents to the EDMS, indexing criteria, or properties, must be completed, offering improvements over document naming limitations associated with shared drive environments.

It is essential to develop routine procedures for saving email messages as the individual conversation string is completed in the course of workflow. Although this approach may result in duplication of content, attempting to construct records in batch mode after the transaction can be labor intensive, haphazard, time consuming and liable to omission of content and other errors. Employees trained to complete standardized index criteria are able to quickly and easily add messages to the EDMS throughout their workflow.

Saving an email message as a document ("save as" to a shared drive or adding to the EDMS) is acceptable as a routine business practice, as it preserves the basic content of the record and the essential properties of sender, recipient and date.

NOTE: A litigation hold notice requires retention of all metadata associated with email.
Section 5 — Records Management in an EDMS

Introduction

Document/record life cycle management is an essential component when planning the implementation of an enterprise document management system (EDMS). This section discusses records management planning considerations and gives an overview of how records management works in an EDMS.

Shared drives, SharePoint sites and email are all components of electronic content management. This section focuses primarily on planning for the use of the FileNet EDMS as the repository for official records.

Users, focused on their business and processes, are typically unfamiliar with records management requirements that begin once their work is completed. Records management in an EDMS involves collaboration between the records administrator, the system administrator and the records custodians on a routine basis to ensure that records in the system are declared, retained and destroyed in accordance with department policy and procedure.

Most of the planning for use of the EDMS involves document organization and employee roles and responsibilities, which have a bearing on how the document life cycle is managed. The remainder of this section discusses records management planning considerations in an EDMS.

Ownership Responsibility and Authority

“Ownership” of records includes the responsibility for their proper security, integrity, retention, and the authority to authorize the destruction of records when they become eligible. It includes the authority to withhold records from destruction when appropriate or necessary. The responsibility and authority typically belong to a management level most directly involved with the official (record copy) records. Determining ownership may involve coordination between offices to determine the appropriate EDMS library for the particular record or document and the level of security for the various users who will have need to access the documents during both active process and inactive retention.

Identifying Record Types

Documents are organized in the EDMS in classes based on business functions. The classes are further subdivided by user-defined record types. A record type must be assigned as a required property, or characteristic, when users save a document to the system. That property, when combined with other document information in a searchable database of document properties, provides a means to manage groups of documents that comprise records.
The record type and document type indexing values developed by business process experts in the various functional areas should be intuitive to employees working with documents in their respective areas. Training and development of written procedures to guide employees is important to assure proper placement of documents in the EDMS.

**Selecting Documents to Add**

The FileNet EDMS is a repository for TxDOT records and documents. Not every document needs to be added to an EDMS. This is particularly true for non-functionally related announcements, copies, emails lacking content, advertising brochures, documents available on the internet or intranet, etc. Developers should establish policy on what their system will contain along with considerations of user rights.

**Managing Drafts or Versions**

Initial EDMS implementations have primarily added final, or completed, documents to the repository as an alternative to filing or storing hard copy. When the EDMS is used to manage document development, it is necessary to consider the management of drafts or versions of documents. In the current EDMS (FileNet Content Services), drafts and versions cannot be separated from the final document for deletion. For sensitive or confidential documents this may represent a risk. In such cases, it may be preferable to use a shared drive or a SharePoint site to develop documents or manage approval processes, and to use the FileNet library as the repository for the final document only.

Written internal policy and procedure may specify the immediate destruction of drafts or versions of documents if their retention is not otherwise required (as in manual or publications development materials in the records retention schedule).

**Declaring a Record**

When planning to use the EDMS for document development or process management, include procedures and the assignment of responsibility for the orderly and timely review of records to initiate retention in the system and to authorize destruction when the records become eligible. For retention and disposition purposes, a document or collection of documents becomes a record at the point it becomes inactive. For example, records managed on a fiscal year basis typically begin their retention at the end of the fiscal year. In an EDMS, the required document status property, such as "Final" or "Completed," in combination with the latest date of the document can be used to establish when it becomes a "record" in the sense the term is meant here. Other properties such as program or project name can associate various component documents in a record.

Use of the required status indexing property when adding finished documents from shared drives or SharePoint sites can also be used to declare a record.
This process should be integrated with other routine file management procedures and include measures such as limiting access rights to protect the integrity of the records during retention. See Chapter 4 for a detailed discussion of record declaration.

Retaining Hard Copy Originals after Scanning

Scanning is a straightforward process and the quality of the scanned image can be verified immediately. Document any requirement to retain the hard copy original for any period after initial scanning in the internal policy and procedural materials governing the operation of the EDMS.

Document Signature Considerations

The Office of General Counsel has determined that electronic approvals authenticated by network logon are satisfactory for internal business processes not otherwise requiring a physical signature. For some business document processes or records, incoming documents bearing signatures and a signed "Final" document (record) may be deemed necessary components of the official record. These should be identified in written procedures governing EDMS use for the affected business area.

Evaluating Archival Needs

A library may eventually contain hundreds of thousands or even millions of documents. In addition to the higher costs of server space and services, such volumes can affect document access and system performance. While conducting routine records management procedures can help control document volumes, libraries will generally trend toward greater document volumes, capacity requirements, and costs. It is important to consider how records retained for lengthy periods of time are actually used and the impact on document handling and workflow when evaluating any alternative strategies/technologies for archiving.

In the TxDOT EDMS system design, there is a status property titled “Reference,” which may be used for documents being retained beyond their eligible destruction date. As a matter of use policy, requiring an owner to explain the use of that property in the document comments field can help subsequent users, authors or owners understand the reason for the extended retention and evaluate the need for continued retention. A separate "Archival Review” status is available for documents that must be retained for State Archives review.

For EDMS implementations involving a significant archival component subject to moderate to frequent retrieval, a FileNet Image Services (IS) library may be better suited to manage a constantly growing document archive. It is a standard online repository which can be accessed using the same client interface as the EDMS. Since the documents reside on a system compatible with the core technology, they will migrate along with the core technology. IS scanning would require different document processing steps and software, but it is still standard within the FileNET application in
TxDOT. Since records destruction is somewhat more complex and expensive in the IS environment, it is not an appropriate technology for records with short retention requirements.

For large archives that are subject to less retrieval activity, acquisition of department-owned mass storage devices may represent a more cost effective archival storage solution.

State Archives Requirements

Certain records cannot be destroyed until they have been reviewed by the State Archives for historical value. These records are identified in the TxDOT records retention schedule and listed in Chapter 10 of this manual. The State Archives is not capable of accepting electronic records, and currently requires state agencies to retain the electronic records indefinitely, unless the agencies are willing to print them out on acid-free paper, or microfilm them for submission to the Archives.

There are relatively few records affected by this requirement, but when they occur in an EDMS, steps to preserve them, either online or converted to offline media must be part of the planning. TxDOT records management can assist in planning a strategy to meet this requirement.

Documenting Procedures

Records management policy and procedures related to an EDMS implementation should be written, dated, and included in general office procedures to establish them as a normal and routine business practice. The procedures should include information related to:

- any special retention requirements (i.e. retention of original documents after scanning),
- frequency of review for destruction,
- an authority list of document owners who can authorize disposition or further retention of records,
- any requirements for documenting why records are withheld from destruction after they become eligible,
- internal policy on archiving and any routine review and purging procedure conducted for records retained under an AV (as long as administratively valuable) retention period.

Records Management Procedures in an EDMS

Records management procedures in an EDMS are the same as those for records in any medium and include steps to:

- ensure secure retention of inactive official records for the appropriate period,
- identify records/documents that are eligible for destruction,
◆ coordinate approval of, or withholding from destruction, by the appropriate authority,
◆ conduct the actual destruction of the records; and
◆ document their destruction.

Assignment of the “Record Type” property when adding a document to the library relates the document to its retention requirement in the TxDOT records retention schedule. The EDMS file plan defines retention rules for each document. Chapter 4, Section 3 contains a detailed discussion of file management in an EDMS.
Section 6 — Risk Management and Electronic Records

Legal Use of Electronic Records

The Texas Rules of Civil Procedure allow the use of electronic records as evidence. Each judge may admit or exclude evidence on the basis of the court's independent evaluation. The court must believe that the records admitted are trustworthy; i.e., that they clearly and accurately relate the facts as originally presented or in summary form. Changes in the Federal Rules of Civil Procedure (FRCP) in recent years have more specifically defined the requirements governing the appropriate management of electronically stored information (ESI) in relation to legal discovery. Penalties for failure to meet those requirements can be severe.

Since electronic records have systemic vulnerabilities, the following basic efforts can help to assure their trustworthiness:

◆ Maintain written procedures related to digital imaging that document the handling of records in the routine course of business. Dated procedures should describe when in the record’s life it is converted, quality control measures employed to verify the digital image, and disposition of the original electronic or hard copy record.

◆ Limit access to documents/records being retained electronically to a single custodian or the system administrator, and establish security measures to prevent alteration of the record content or properties.

◆ Maintaining a current records retention schedule can have an important impact on court proceedings by documenting a record's existence and retention period. The fact that a record is on the schedule shows that the department produces it regularly. Refer to Chapter 3, Records Retention Schedule, for procedures to update the schedule.

◆ Consistently maintain a records disposition log. Courts generally accept the defense that records have been destroyed under an approved records retention schedule. This is an especially effective defense if there is documentation over a period of time to prove that the records have been routinely destroyed in compliance with the retention period specified on the schedule. See Chapter 10, Records Destruction for procedures related to completing Form 1420, Records Destruction Log.

◆ Keep records to establish equipment and software reliability. A daily operations log indicating the absence of any malfunctions is generally adequate. Since a record's contents may change if equipment is not operating properly, evidence that the equipment was operating reliably on the day an electronic record was prepared may be required. Record contents may also be affected by computer program errors. Evidence related to program code development, revision and testing documentation might be required. An expert may examine the program to determine accuracy and reliability. The specific version of the program used to process the electronic record being entered into evidence may be required. A different version of the program may be
considered if it is the only one available. However, the absence of the exact version may raise serious questions about the trustworthiness of the record.

- Printouts prepared in the ordinary course of business may be perceived as more trustworthy than printouts prepared for trial, although courts have become more accepting of records in their original electronic format. Printouts can serve as an audit trail documenting data integrity, even though time has elapsed between creation and printing of the record.

**Email Best Practices**

Some simple common-sense measures, used in concert with the techniques for email management described in Section 4, can help reduce the expense involved in searching emails for discovery or open records requests. Additional recommendations are published in a best practices document in the IT intranet site.

- Dispose of purely transitory emails as soon as they have served their purpose.
- Include management of email records in employee performance planning and evaluation as appropriate.
- Maintain a short auto delete and backup interval (recommend 30 days).
- Limit the number of recipients to as few as possible and avoid replying to “All Recipients” unless needs require it.
- Include specific identifying information such as ROW Parcel Number, County CSJ Number, Purchase Order Number, etc. in the subject line.

The following guidelines can help reduce potential negative impacts related to email:

- Establish a use policy on when to call or meet personally instead of using email, considering
  - sensitive or confidential subject matter or content, and
  - complicated or nuanced content.
- Content to avoid:
  - off-color jokes or sexual content—may be viewed as sexual harassment
  - sensitive or confidential information
  - political opinion or commentary—may be viewed as breach of lobbying ethics
  - discriminatory content against any protected group
  - chain email or forwarded jokes
  - legal jargon (lawyer-speak)
  - messages that vent or complain
  - messages admitting fault or liability
- Content precautions:
Be careful when expressing opinions to external recipients (such as vendors and the general public), as the viewpoint may be construed as official or state policy or, in some cases, as an implied contract.

Be cautious when expressing personal criticism or opinions, as unintended wide distributions may result.

Be very careful with informality or humor. Without the benefit of inflection and visual cues, what may be humorous in one context can appear otherwise in print. Your recipient may understand, but the content could appear quite differently when presented as evidence.

As a general rule, avoid content your supervisor would consider unacceptable or content you wouldn’t want to see associated with your name in the news.

Preparing for Electronic Discovery

The Office of General Counsel (OGC) issues policy and procedures for litigation holds. When OGC issues a litigation hold notice to preserve documents relevant to a case, routine document retention/destruction policy is suspended to insure the preservation of relevant documents.

A litigation hold notice does not require immediate production of records. What it does require is:

- **Location and identification of all relevant records/documents in any medium.** Current file plans and Record Copy Responsibility Lists can help to locate the records. This step can also include locating records on backup media, portable devices or voice mail.

- **Preservation and retention** of relevant electronic documents in their native application to preserve document metadata. If documents were routinely scanned or otherwise retained in a way that lost the electronic metadata before the litigation hold, there is no need to attempt to reconstruct them. Electronic records existing in their native applications at the time the litigation hold is issued, or created subsequent to the litigation hold, must be preserved in their native application.

- **Security** measures are required to preserve the authenticity and integrity of the electronic records.
Chapter 6 — Vital Records

Contents:

Section 1 — Identifying Vital Records
Section 2 — Threats and Protection
Section 1 — Identifying Vital Records

Vital Records

Vital (essential) records, as defined in the Preservation of Essential Records Act Texas Government Code, §441.056, are records that, following a disaster, are necessary for the department to

- resume or continue operations;
- reaffirm authority and activity, including legal and financial positions; and
- protect the rights and interests of the department and its customers.

Although all state records serve a purpose, only about 5 percent of an agency's records are truly vital as defined above.

The Act requires each state agency to identify vital records, and to be able to rapidly reconstruct vital records from backup copies after a disaster. This chapter contains information on identifying and protecting vital records.

Chapter 7, "Disaster Recovery Planning," describes procedures that can help to reconstruct records quickly following a disaster.

Identifying Vital Records

Vital records are only those records that are essential for TxDOT offices to carry out their responsibilities following a disaster. Vital records are identified in the TxDOT records retention schedule.

Vital records may consist of

- operational records necessary to resume or continue operations;
- legal records for proof of authority or activity;
- fiscal/financial records, especially those related to receivables; and/or
- governmental records necessary to protect the rights and interests of the department, its employees and the public.

Responsibility for Vital Records

Offices that maintain vital records are responsible for

- identifying vital records and making sure they are listed as vital on the TxDOT Records retention schedule,
- implementing vital records protection procedures to back up vital records, and
advising the TxDOT records management officer on backup records locations, contacts and sources for records retrieval and reconstruction.

Common Vital Records

Vital records are not necessarily permanent records or records with archival value. Vital records may be vital for only a part of their total retention.

Common vital records include the following:

- active contracts and agreements, with all amendments and supporting documentation
- financial records
  - accounts receivable (vendors will provide copies of lost or damaged accounts payable)
  - loans or money transactions
  - general ledgers
  - records proving payment
- employee records
  - payroll
  - benefits
- operations and manufacturing records
  - engineering drawings
  - in-process project records
  - research and development notes, reports, plans, formulae
  - production/design specifications
  - equipment inventory
- negotiable instruments
  - checks
  - bonds
  - notes
- ownership records
  - deeds
  - titles
  - leases
  - patents and trademarks
  - licenses
◆ insurance policy information

If a record you consider vital is not identified as vital on the records retention schedule, annotate your file plan or record copy responsibility list to make employees aware of the need for special handling for the records. You may also include the following:

◆ **Special instructions.** For example, the record may be vital only for a specific period of time within a longer retention period.

◆ **Backup protection.** If the backup protection method is dispersal through *routine* distribution, indicate the department offices that are the primary and secondary contacts. For districts, this may include both a building within the district and an area office or Austin headquarters division which may have a copy as part of routine operations. If the record is dispersed through *planned* distribution, indicate the location of the backup copy. Additionally, note any special storage equipment used and its specifications.

◆ **Persons authorized to access the records.** If the records are kept in secured storage, include information on contact persons for access.
Section 2 — Threats and Protection

Introduction

This section contains information on
◆ potential threats to records,
◆ methods of protection,
◆ storage equipment and conditions.

Potential Threats to Records

Potential threats to records include the following:
◆ fire
◆ water
◆ theft and sabotage
◆ natural disaster
◆ civil disaster
◆ accidental destruction
◆ neglect
◆ misplacement
◆ age
### Methods of Records Protection

Offices with record copy responsibility for vital records are responsible for taking measures to protect those records. Four effective methods of protection in the order of their expense are

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Duplication and Dispersal     | Dispersal is the practice of maintaining copies of a vital record in more than one location on the assumption that a disaster is unlikely to affect two different locations at the same time. There are two types of dispersal: routine and planned. Either way, you should document specific remote storage locations in disaster recovery procedures (see Chapter 7, “Disaster Recovery Planning.”)  
  - Routine dispersal is frequently used in an agency with more than one office location. In the course of regular business, vital records are sent to several different locations for use and reference. As long as these records are maintained at two or more locations, **and**, as long as employees are aware that the records are vital, additional protection may not be required.  
  - Planned dispersal is the distribution of a copy of a vital record specifically for protection purposes. The copy can be in any medium or format. The copy is sent to another storage location until the records are no longer considered vital or retention requirements are met.  
  - Periodic inspection and duplication can arrest the aging process to some degree.                                                                                                                                                                                                 |
| On-site Storage               | On-site storage involves storing backup copies in special storage equipment in or near the office location. Fire-resistant files or vaults are used most often. Use storage equipment designed specifically for the record medium (paper, film, electronic) and use it only for vital records. Place equipment carefully, with disaster prevention in mind. Equipment should be on an outside wall, if possible. In fires, structures tend to collapse toward the center, where the fire burns hotter and longer. Do not store vital records in a basement. Basements collect water from efforts to extinguish fires, and flooding is an obvious danger. |
| Off-site Storage              | Off-site storage involves storing backup copies in a remote location and is best for records that are referenced infrequently. Off-site storage locations in Austin include TxDOT’s records center and the State Records Center. Districts may develop storage areas or choose to use a commercial off-site storage facility. Considerations in selecting a commercial facility include the following:  
  - speed of access to the records  
  - access control and security at the facility  
  - environmental conditions (temperature, humidity, protection from outside air infiltration and electromagnetic fields, insect and rodent control) related to the type of record media stored  
  - whether the facility meets American National Standard Institute standards for storage  
  - availability of auxiliary power to maintain environmental conditions in the event of utility power failure  
  - availability of insurance for the center and the records  
  - type of fire prevention, detection and suppression systems used  
  - type of filing index system used  
  - procedures for receipt, transfer and disposal of records  
  - existence of an established disaster recovery plan  
  - availability of duplication and reproduction equipment  
  - client references.                                                                                                                                                                                                                                                                 |

---

*Records Management 6-6 TxDOT 12/2014*
Records protection equipment, such as fire resistant file cabinets, safes or vaults, is rated for safety and damage resistance. Labels on the equipment certify that it has been tested for its capacity to withstand specified levels of intense heat, sudden cooling and severe impact.

The American National Standards Institute (ANSI), National Fire Protection Association (NFPA), and the Underwriters' Laboratories, Inc. (UL) have established standards for the storage of records media.

Damage begins when temperature and humidity exceed the following levels:

### Record Damage Thresholds

<table>
<thead>
<tr>
<th>Medium</th>
<th>Temperature</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>350º F</td>
<td>100%</td>
</tr>
<tr>
<td>Microfilm (silver base)</td>
<td>150º F</td>
<td>85%</td>
</tr>
<tr>
<td>Magnetic</td>
<td>150º F</td>
<td>85%</td>
</tr>
</tbody>
</table>

NOTE: Optical media are environmentally more tolerant than other media.

### Ideal Storage Conditions

<table>
<thead>
<tr>
<th>Medium</th>
<th>Temperature</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>60-70º F</td>
<td>50-60%</td>
</tr>
<tr>
<td>Microfilm (silver base)</td>
<td>65-70º F</td>
<td>20-30%</td>
</tr>
<tr>
<td>Magnetic</td>
<td>65-75º F</td>
<td>30-50%</td>
</tr>
<tr>
<td>Optical</td>
<td>14-122º F</td>
<td>10-90%</td>
</tr>
</tbody>
</table>
Mark all vital records storage containers to indicate the vital status of their contents.
Chapter 7 — Disaster Recovery Planning

Contents:

Section 1 — Overview
Section 2 — Disaster Prevention
Section 3 — Developing a Disaster Recovery Plan
Section 4 — Disaster Recovery Plan Checklist
Section 1 — Overview

General -- Steps in Disaster Recovery Planning

Disaster recovery planning includes the following steps:

- disaster prevention measures
- development of a disaster recovery plan
- development of disaster recovery and records salvage procedures, as part of the plan

Definitions

A disaster is generally defined as an event that causes widespread destruction and distress.

When a disaster causes the irreparable loss of information, it may be called a catastrophe. This chapter contains information that can help prevent disasters and help to keep any that may occur from becoming catastrophes.
Recognizing Threats to Records

Recognizing potential threats to records can help prevent disasters. The four most common threats to records include the following:

- fire
- water
- theft and sabotage
- adverse environmental conditions
  - flood
  - tornado or hurricane
  - earthquake

Other threats include the following:

- civil disaster
- accidental destruction
- neglect
- misplacement
- deterioration by age
Methods of Protection

The table below lists the four most common threats to records and ways to protect records from damage.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Protection</th>
</tr>
</thead>
</table>
| **Fire** | To minimize chances that a fire will start and maximize chances for quickly extinguishing any fires that do start:  
- Do not store records near a heater, radiator or other heat source.  
- Prohibit smoking in record storage areas.  
- Do not store records with chemicals, cleaning supplies, etc.  
- Remove paper clutter from storage areas.  
- Observe approved records retention periods to ensure the timely destruction and removal of records, thereby reducing the amount of potential fuel.  
- Make sure electrical wiring is safe. When possible, avoid the extended use of lighting or equipment with cords around storage areas. After using such appliances, unplug them before leaving the area.  
- Comply with all local fire, electrical, plumbing, heating and construction codes.  
- Have fire extinguishers available near the records. Have them inspected regularly, and train staff to know where they are located and how to use them.  
- Clearly mark escape routes and exits. Hold regular fire drills to practice emergency procedures.  
- Periodically evaluate fire prevention systems in use, such as smoke detectors and/or sprinkler systems.  
- Try to store records against an outside wall. In fires, structures tend to collapse toward the center where fire burns hottest and longest. |
| **Water** | Water damage may occur as a result of other forms of disaster. Water damage and flooding often occur as a result of efforts to put out a fire. Winds and wind-driven rain can break windows and damage records. Also, routine structural failures such as backed-up drains and sewers, or broken pipes, can cause water damage. To reduce the likelihood of water damage to records, do the following:  
- Avoid storing records in basements, under water pipes, or directly on the floor.  
- Locate all drains and have them checked regularly.  
- Regularly inspect the sprinkler system, and check the general condition of the records storage site for susceptibility to flooding.  
- Look for any potential water hazards during routine inspections of plumbing.  
- Do not install carpet in storage areas. It retains moisture, prevents drainage and, if wet, will create humidity and temperature problems.  
- Try to store records in an area without windows. |
## Theft and Sabotage

Security is the key to protecting records from theft and sabotage. Consider the following when determining who will have access to individual record series:

- whether the records are classified as open or confidential
- characteristics of the record medium
- whether the records include vital records
- physical features of the building where the records are used or stored

Conduct an initial security analysis and periodic evaluations of security in records storage areas and active files areas. The following basic protective measures will improve security:

- Determine who needs access to specific record series and limit the number of employees who handle these records.
- Limit access to record storage areas.
- Be aware that terminated employees may pose security risks. Be sure they turn in all relevant identification and keys before leaving.
- Ensure that all access control systems, intrusion detection systems and alarm systems receive regular maintenance.
- Make security checks at closing time to ensure all exits and windows are locked, all equipment has been turned off or unplugged, all lights and water faucets are off, no cigarettes are smoldering in ashtrays and no unauthorized persons are in the building.
- Keep the exterior of the facility well lit at night.
- Establish procedures to follow in the event of theft or vandalism.

## Environmental Conditions

The most important factor in protection from environmental conditions is avoidance of extremes. Avoid storing records in attics, basements or warehouses that are not in some way climatically controlled. To help retard natural deterioration, provide at least the following:

- air-conditioning
- air circulation
- temperature stabilized within a range of 60-75 degrees Fahrenheit

Most modern paper deteriorates continuously due to high levels of paper acidity. Atmospheric pollution intensifies this problem. Microforms and magnetic media may deteriorate unless there are controls for temperature, humidity, pollution and light. Some protective measures in addition to the above are to

- avoid storing records in areas where there is smoke, dust or chemical fumes produced by paints or copying devices,
- protect all records from direct sunlight and bright lights,
- keep the storage area free of food, beverages and plants to avoid soiling the records or attracting insects or rodents.

### Record Threats and Methods of Protection

<table>
<thead>
<tr>
<th>Threat</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft and Sabotage</td>
<td>Security is the key to protecting records from theft and sabotage. Consider the following when</td>
</tr>
<tr>
<td></td>
<td>determining who will have access to individual record series:</td>
</tr>
<tr>
<td></td>
<td>✦ whether the records are classified as open or confidential</td>
</tr>
<tr>
<td></td>
<td>✦ characteristics of the record medium</td>
</tr>
<tr>
<td></td>
<td>✦ whether the records include vital records</td>
</tr>
<tr>
<td></td>
<td>✦ physical features of the building where the records are used or stored</td>
</tr>
<tr>
<td></td>
<td>Conduct an initial security analysis and periodic evaluations of security in records storage</td>
</tr>
<tr>
<td></td>
<td>areas and active files areas. The following basic protective measures will improve security:</td>
</tr>
<tr>
<td></td>
<td>✦ Determine who needs access to specific record series and limit the number of employees who</td>
</tr>
<tr>
<td></td>
<td>handle these records.</td>
</tr>
<tr>
<td></td>
<td>✦ Limit access to record storage areas.</td>
</tr>
<tr>
<td></td>
<td>✦ Be aware that terminated employees may pose security risks. Be sure they turn in all relevant</td>
</tr>
<tr>
<td></td>
<td>identification and keys before leaving.</td>
</tr>
<tr>
<td></td>
<td>✦ Ensure that all access control systems, intrusion detection systems and alarm systems receive</td>
</tr>
<tr>
<td></td>
<td>regular maintenance.</td>
</tr>
<tr>
<td></td>
<td>✦ Make security checks at closing time to ensure all exits and windows are locked, all equipment</td>
</tr>
<tr>
<td></td>
<td>has been turned off or unplugged, all lights and water faucets are off, no cigarettes are</td>
</tr>
<tr>
<td></td>
<td>smoldering in ashtrays and no unauthorized persons are in the building.</td>
</tr>
<tr>
<td></td>
<td>✦ Keep the exterior of the facility well lit at night.</td>
</tr>
<tr>
<td>Environmental Conditions</td>
<td>Establish procedures to follow in the event of theft or vandalism.</td>
</tr>
<tr>
<td></td>
<td>The most important factor in protection from environmental conditions is avoidance of extremes.</td>
</tr>
<tr>
<td></td>
<td>Avoid storing records in attics, basements or warehouses that are not in some way climatically</td>
</tr>
<tr>
<td></td>
<td>controlled. To help retard natural deterioration, provide at least the following:</td>
</tr>
<tr>
<td></td>
<td>✦ air-conditioning</td>
</tr>
<tr>
<td></td>
<td>✦ air circulation</td>
</tr>
<tr>
<td></td>
<td>✦ temperature stabilized within a range of 60-75 degrees Fahrenheit</td>
</tr>
<tr>
<td></td>
<td>Most modern paper deteriorates continuously due to high levels of paper acidity. Atmospheric</td>
</tr>
<tr>
<td></td>
<td>pollution intensifies this problem. Microforms and magnetic media may deteriorate unless there</td>
</tr>
<tr>
<td></td>
<td>are controls for temperature, humidity, pollution and light. Some protective measures in addition</td>
</tr>
<tr>
<td></td>
<td>to the above are to</td>
</tr>
<tr>
<td></td>
<td>✦ avoid storing records in areas where there is smoke, dust or chemical fumes produced by</td>
</tr>
<tr>
<td></td>
<td>paints or copying devices,</td>
</tr>
<tr>
<td></td>
<td>✦ protect all records from direct sunlight and bright lights,</td>
</tr>
<tr>
<td></td>
<td>✦ keep the storage area free of food, beverages and plants to avoid soiling the records or</td>
</tr>
<tr>
<td></td>
<td>attracting insects or rodents.</td>
</tr>
</tbody>
</table>
Section 3 — Developing a Disaster Recovery Plan

General — What the Plan Involves

Districts, divisions, and offices should develop a written disaster recovery plan appropriate to their own operations. Even minimal preparation can have a significant impact on the success of efforts to recover TxDOT records.

The following pages contain information to use in developing a disaster recovery plan. A link to a downloadable worksheet is provided in Section 4, "Disaster Recovery Plan Checklist" of this chapter.

Developing a disaster recovery plan involves
- stockpiling emergency supplies and arranging services,
- establishing a disaster recovery team,
- developing disaster recovery and records salvage procedures,
- contingency planning.

Emergency Supplies and Services

In an emergency, self-reliance is critical. In any major disaster, TxDOT is likely to have to assist with recovery efforts for other agencies and the public while managing its own recovery.

Initial disaster recovery plan development should include:
- stockpiling emergency supplies,
- arranging necessary services to aid in disaster recovery.

Check supplies and re-confirm service agreements periodically. After a wide-scale disaster, these resources may not be readily available. Suppliers or service organizations may have their own damages to deal with, or they may be helping someone else.

Disaster Recovery Team

Department offices should establish in-house disaster recovery teams to resume or sustain operations after a disaster, including handling recovery of their records. The teams should develop and practice disaster recovery and records salvage procedures. Teams may also want to train office employees in disaster recovery.
Each team member should have two copies of the office's disaster recovery plan, one at the office and another at home.

Recovery Team Responsibilities

Ideally, a disaster recovery team should consist of at least four members, including a team leader. Each team member should have an alternate. Responsibilities of team members are as follows:

◆ Team leader: Acts as point of contact for local emergency service agencies; performs overall management of the team's disaster recovery and records salvage procedures; coordinates with other offices; authorizes expenditures for wages, supplies, transportation and services; and is liaison with TxDOT customers and/or the public.

◆ Recovery and salvage supervisor: Assembles, trains, and directs work crews for recovery and salvage procedures. Controls the flow of work and materials.

◆ Coordinator of Enterprise Content and Records Management, (ECRM): Assembles supplies and equipment and may arrange such things as food for work crews.

◆ Record keeper: Inventories damaged records. Assesses damage and salvage required. Performs or supervises recovery and salvage procedures.

Disaster Recovery and Records Salvage Procedures

Each district, division and office is responsible for developing emergency procedures to follow in a disaster and making sure employees are familiar with them.

Include these essential procedures in any disaster recovery plan:

1. **Activate Recovery Team** - Once the building has been declared safe to enter, the team leader should contact the team and brief them on procedures and priorities to be met. The recovery team should then

   ◆ assign specific responsibilities to members;
   ◆ set up a communications center and obtain services, supplies and equipment;
   ◆ make arrangements to take care of physical needs (food, water, hygiene) of personnel involved in the recovery.

2. **Establish Security and Safety** - For security and safety, restrict access to damaged area(s), allowing only essential personnel to enter. This minimizes opportunities for further damage to records and injuries to personnel. Use security guards, sign-in/out registers, and/or identification badges to restrict access.

   Basic safety precautions include the following:

   ◆ Inspect disaster areas for hidden hazards, such as shorted motors or broken electrical wires.
Avoid standing water and wet carpets, which make it dangerous to use electrical equipment.

Install and use temporary wiring properly.

Handle fire- or water-damaged files carefully. Wet records are heavy and fragile. Use care lifting record boxes or opening file cabinets.

Use face masks and protective gloves. Wash or clean clothing as soon as possible to reduce health hazards from fungi and bacteria.

3. Assess Damage - Inspect damaged areas as quickly as possible. Avoid handling records, if possible. Take photos to document record damage. Keep the following questions in mind:

- How much damage has occurred?
- What kind (fire, smoke, soot, clean or dirty water, heat, humidity)?
- Is it confined to one area or is the entire building damaged?
- How much of the records holdings are affected?
- What type(s) of records media have been damaged (paper, microforms, photographs, magnetic tapes, diskettes)?
- Are the damaged records easily replaced? (Are backup copies stored off-site? Are the damaged records convenience copies? Can they be replaced with copies from other offices?)
- If the damaged records are irreplaceable, what is their value? (How important are these records to the business of TxDOT?)
- What is the order of priority to recover damaged essential records?
- Can the in-house recovery team salvage records or is outside help needed?

NOTE: Take steps to stabilize the environment while assessing the damage (see below).

4. Stabilize Environment - Take steps to stabilize the environment while the damage assessment is taking place. Mold can appear on records in 48 hours and is encouraged by high humidity and temperatures. Quickly reducing the humidity and temperature can reduce the risk of mold and buy time for recovery.

The following procedures will help stabilize the environment:

- Keep the air constantly circulating.
- Arrange fans to expel humid air outside.
- Use dehumidifiers if they are helpful. (Dehumidifiers may help in small, enclosed areas. Operating them may raise the temperature, however, and they tend to freeze up in colder temperatures.)
Immediately pump standing water from the area. Use caution -- standing water can conceal hazards. Remove wet debris and carpeting. The following equipment should be readily accessible:

- portable generators, in case of power failure
- shop vacuums capable of handling water (pumps may be needed to remove large quantities of standing water)
- fans to circulate the air
- thermometers, hygrometers or other tools to measure temperature and humidity

5. Treat Water-Damaged Records - Water-damaged records are the records most likely to be salvaged. See the next table for methods of treating water-damaged records.

6. Perform Post-Disaster Assessment - Assessing the disaster recovery plan is essential. Share the results with districts, divisions and offices and revise the plan if needed. Assess the following:

- effectiveness of recovery procedures
- areas for improvement
- sources and supplies
- any off-site facilities used

Salvaging Water-Damaged Records

The records most likely to be salvaged after a disaster are those that have water damage. A number of options are available for treating water-damaged records. The steps to follow vary according to the record medium and are described below.

Paper - When paper records are slightly damp, air-drying (natural drying) may suffice. If records are soaked, they should be freeze-dried, regardless of quantity.

- Air-drying: To air-dry paper records, hang the paper on lines. You may want to interleave pages with special blotter paper as a preliminary step before hanging the paper.
- Rooms used for drying areas should have good air circulation and low humidity. Use fans, dehumidifiers and/or air conditioning. Handheld hair dryers (set on cool) may be used to speed drying.
- Freeze-drying: The most effective procedure for stabilizing water-damaged records and archival materials is to blast-freeze them to a temperature of -20 degrees F, and then dry them using a thermal vacuum process.

Freezing allows time to estimate recovery costs, prepare and coordinate subsequent steps in the drying and recovery operation, and clean up the disaster site. In addition, freezing stabilizes water-soluble materials (inks, dyes, etc.), that may disperse during air drying.
Thermal vacuum drying causes water to pass from a frozen state to a vapor without returning to a liquid form. It reduces stains and removes the odor caused by smoke. Determining a source for thermal-vacuum drying services should be part of disaster planning. The Blackmon-Mooring Steamatic company (in Austin) has special vehicles that can travel to remote sites to perform this service. (Many carpet cleaning/water removal services can perform the service or suggest vendors who can.)

**Microfilm** - In recovering microfilm or microfiche, speed is essential to avoid the breakdown of film emulsions and the onset of bacterial growth which destroys images.

Immerse the film in clean, cold, preferably distilled water. Send the film to a professional laboratory for cleaning. Generally, film should not be frozen because ice crystals may harm it.

**Electronic Media** - Off-site storage of backups is the best possible disaster recovery strategy for electronic records. If electronic records on portable media are water-damaged, do not use them until they are thoroughly clean and dry and their housing or containers have been replaced. This reduces the possibility of damage to equipment, especially for disk drives.

**Diskettes** require the following steps:
- To clean and dry, do the following:
  - Drain.
  - Remove from jackets.
  - Rinse in distilled water.
  - Blot with lint-free cloth.
  - Air-dry approximately eight hours.
- When diskettes are dry, do the following:
  - Insert into a new jacket.
  - Copy information on damaged diskettes onto new diskettes.
  - If information copies correctly, discard damaged diskettes.
  - Clean copy equipment drive heads to prevent permanent damage to the heads.

**Magnetic Tape** that has become wet has a good chance for recovery through these steps:
- Hand dry all external surfaces with a soft, lint-free cloth.
- Air-dry the tape using a tape cleaner or winder to run the tape from reel to reel.
- Consult a company that does magnetic tape restoration.

**Compact Disk or other Optical Media** require these steps:
- Clean any dirt or debris from the disk using a disk cleaning solution.
Contingency Planning

Contingency planning combines emergency preparation with routine office procedures to help the office continue operations with as little interruption as possible after a disaster.

The real disaster is failure to prevent avoidable situations.

For effective contingency planning, do the following:

◆ Keep your office file plan up-to-date. Know which records your office has record copy responsibility for, and be ready to carry out disaster recovery and salvage procedures for those records.

◆ Be aware of alternate locations for records. You may use this information to replace records quickly after a disaster. District and division offices that are related by function are often alternate locations for the same record, even though only one office may be designated as the office of record. Part of a disaster preparedness plan could include:
  ● notation of alternate locations on the file plan, or
  ● securing a copy of any procedures manual or internal office procedural material that may include information on alternate locations for records.

◆ Keep a current list of contact persons for various types of records.

◆ Keep identification and protections for vital records current. Carry out vital records protection as described in Chapter 6, "Vital Records" in a disciplined manner.

◆ Back up electronic records routinely and frequently. Dispersal of a second backup copy at another, off-site location is a good protective measure.
Section 4 — Disaster Recovery Plan Checklist

General

This section consists of a checklist of information that may be helpful for offices to include when preparing a disaster recovery plan. Click here to access a checklist Word document for your use.

Any written plan should be dated each time it is revised to show its currency. Plans should be reviewed and updated on a regular, periodic basis.

Initial Contact to Call in the Event of a Disaster:

Each district, division and office (and individual offices within them) should establish a point of initial contact for disaster reporting and initiation of disaster recovery efforts.

Disaster Recovery Team:

A disaster recovery team should be appointed to manage recovery efforts. It is useful to develop a "telephone tree" to arrange who is to call whom on discovery of a disaster.

Emergency Services to be Called in the Event of a Disaster:

Maintain a directory of emergency services to be contacted in the event of a disaster.

Locations of In-House Emergency Equipment and Supplies

It may be helpful to include a map or floor plan with the location of emergency equipment and supplies marked as part of the disaster recovery plan. Location may actually be the office for which the plan is being developed or in another department building that is accessible.

Sources of Off-Site Equipment and Supplies

Use a separate list for off-site equipment and supplies. If any of the items are maintained on-site, modify your location table and note the location.

Salvage Priority List

To quickly identify and prioritize records to recover, attach a copy of the office's file plan. This attachment should identify all vital record series for which your office has departmental record
copy responsibility. You may also wish to identify non-vital record series that should be recovered in order for the office to resume or continue operations immediately.

Note on the file plan the location and record medium of the backup copy for each vital record series. Note offices and contacts for non-vital records necessary to continue business.

Assign each vital and non-vital record series a salvage priority using numerical values:

1. Salvage at all costs (records of historical value or non-vital records that are important to TxDOT operations and would be difficult to reconstruct).
2. Salvage if time and resources permit (records that are of less importance or that would be easier to recreate than those with a priority).
3. Dispose of as part of general cleanup (examples are convenience copies with the record copy at another location).

The following questions will help you determine salvage priority:

1. Are the records duplicated elsewhere?
2. Can the records be replaced? At what cost?
3. Would it cost more to replace or restore the records?
4. How important are the records to TxDOT?

Follow-Up Assessment

After recovery, prepare a written report assessing the effectiveness of your office's disaster recovery plan. Include photographs. Note the plan's effectiveness and evaluate sources of supplies, equipment and any off-site services or facilities used. Attach the report to a copy of the disaster recovery plan used.

Modify and/or update the plan as needed.
Chapter 8 — Inactive Record Storage

Contents:

Section 1 — Overview
Section 2 — Transferring Records to Storage
Section 3 — Transmittal and Storage Documentation
Section 4 — Receipt and Storage Location
Section 5 — Retrieving Records
Section 6 — Storage Areas and Equipment
Section 1 — Overview

Introduction

This chapter contains guidelines and procedures for inactive hard copy records storage.

Generally, only active records need to be maintained in office space. A common measure for identifying active records is one reference per month per file or file drawer. Records kept for a specific period of time during which they are most likely to be referenced, (for example, the current fiscal year) may also be considered as active.

Proper implementation of the TxDOT records retention schedule and use of inactive records storage

◆ reduces the volume of records and the equipment and space needed to accommodate them,
◆ increases the filing and retrieval efficiency in the office,
◆ minimizes the cost of storing official department records for the required retention period,
◆ preserves accessibility to records during their required retention periods, and
◆ ensures proper coordination and documentation of the destruction of official state records.

Records Eligible for Storage at a Records Center

Only official record copy records or files of Austin headquarters divisions and offices listed on the TxDOT records retention schedule are eligible for storage at a the records center. Districts should maintain a similar policy for storing records to conserve resources.

Information or convenience records or files are ineligible for storage, since they can be disposed of without formality once their administrative value has been met.

A record series with a retention code of AV (as long as administratively valuable) is not eligible for records center storage unless a specific retention period and destruction date is assigned to it.

For assistance contact TxDOT Records Management by e-mail from the link on the records management intranet site or at the phone number on the site.

Storage Locations

Eligible records from headquarters divisions or offices are stored at the TxDOT records center at 2000-A Centimeter Circle in north Austin.

Districts may store inactive records locally or at off-site storage facilities.
Selecting Records for Storage

Points to consider when evaluating whether to transfer records to storage include:

- volume of records and required minimum retention period
- how frequently the records are needed or used
- the urgency of need when they are required
- time required for retrieval
- availability, cost and use of office space and filing equipment vs. the lower cost of storage
- viability of imaging (in Chapter 9, Section 1, Storing, Scanning or Microfilming?) as an alternative to hard copy storage.
Section 2 — Transferring Records to Storage

Procedural Overview

Transferring records to storage involves:

◆ boxing records in an approved storage box,
◆ completing transmittal or stored records index documentation to include:
  ● indexing the records in sufficient detail to enable efficient retrieval,
  ● including reference to their Agency Item Number on the TxDOT Records retention schedule, which is necessary in documenting their destruction and (in Austin) verifying eligibility for storage,
  ● noting the date the records will be eligible for destruction,
  ● noting any records with a State Archives review requirement,
◆ marking the boxes with identification of their storage location, and
◆ indicating the storage location on the stored records index or transmittal.

Districts may choose to use the department’s Form 1419, Records Transmittal, available on the EForms intranet site and described in the next section, for the indexing, or they may develop their own documentation. Headquarters divisions and offices must follow the procedures in the table below to obtain records storage services.
Division and Office Procedure

Headquarters Division and Office Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that records are eligible for storage: Only record copies are eligible for inactive storage at a records center. If you have questions, contact records management at (512) 374-5203 or by e-mailing GSD_Records_Management.</td>
</tr>
<tr>
<td>2</td>
<td>Order standard document storage boxes (NIGP # 615-37-13-0850) through supply rooms, warehouses or Regional Distribution Centers.</td>
</tr>
<tr>
<td>3</td>
<td>Prepare records for transfer. Remove extra copies, routing slips and any other material not to be retained. Leave records in their original file folders and sequence. It may be helpful to include file guides from the original files.</td>
</tr>
</tbody>
</table>
| 4    | Pack boxes. Each box holds 13 inches of letter-size, or 10 inches of legal-size records, with 2 inches of handling room.  
  ◆ Pack only one record series to a box.  
  ◆ Pack only records with the same destruction date in a box.  
  ◆ Be sure to leave handling room. Do not overstuff boxes.  
  **NOTE:** While packing, complete the Records Series Title block and Description & Date of Records block on Form 1419, Records Transfer and Service Request Form. |
| 5    | Number boxes sequentially beginning with 1. Mark the number (about one inch high) to the left of the handhold cutout on the box end. Be sure to do the following:  
  ◆ Number the box, not the lid, because lids are interchangeable.  
  ◆ Do not write any other information on the box.  
  ◆ Make sure the numbers correspond to how boxes are listed on Form 1419 (see below). |
| 6    | Complete Form 1419, Records Transmittal. Detailed instructions for completing the form are included with the electronic version. Section 3 also contains the instructions.  
After completing the form,  
  ◆ keep a copy of the form for your files,  
  ◆ place the original Form 1419 on top of the records in box 1,  
  ◆ do not tape lids to boxes. |
| 7    | Ship boxes to storage. Austin headquarters divisions and offices use interoffice mail if there are five or fewer boxes. For larger quantities, call (512) 465-7390, to arrange shipment to Records Management, 2000-B Centimeter Circle.  
If there are enough boxes to ship on a pallet, do the following:  
  ◆ Secure box lids with tape.  
  ◆ Stack boxes no more than six high.  
  ◆ Stack boxes in numerical order, top to bottom, left to right.  
  ◆ If boxes are stacked more than four high, it is a good idea to shrink-wrap them. |

Proper Packaging and Documentation

Records will be returned to the sender if they are sent for storage

◆ in any container other than the standard document box (NIGP # 615-37-13-0850)
◆ in a container bearing any markings other than the box number, as indicated in step 5 of the procedures above, and/or
◆ with an inaccurate or incomplete Form 1419, Records Transmittal.
◆ Districts may find it convenient to mark identifying information on the outside of boxes being retained locally. If archival records will ultimately be forwarded to records management for handling with the State Archives, the boxes must be kept clean or the records will have to be re-boxed before shipping.
Section 3 — Transmittal and Storage Documentation

Uses of Form 1419, Records Transmittal

Headquarters divisions and offices sending records for storage or destruction must use Form 1419, Records Transmittal, which

◆ serves as a manifest for records in transit to verify that all records shipped are received,
◆ serves as an index and locator for records in storage,
◆ is used to provide the office of primary responsibility (OPR) a detail listing when destruction of the records is coordinated, and
◆ provides an audit trail to document the storage and disposition of official state records in accordance with the agency's approved records retention schedule.

Instructions for Completing Form 1419

One Form 1419 can be used to transmit a number of boxes of records. Although you may transmit multiple boxes with varying destruction dates with a single Form 1419, records management recommends transmitting a single record series with a single destruction date with each Form 1419 to reduce the possibility of confusion or errors. Following is an example of a completed Form 1419, Records Transmittal.
The following table describes the blocks on the form and the information necessary to complete it.

### How To Complete Form 1419

<table>
<thead>
<tr>
<th>Step</th>
<th>Block Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Division, Section/Location</td>
<td>Enter the complete return address of the sender. Include district, division or office, section and location. It is a good idea to note the phone number of the sending office's records coordinator.</td>
</tr>
<tr>
<td>2</td>
<td>Individual Receiving Records</td>
<td>Leave blank. Completed by recipient.</td>
</tr>
<tr>
<td>3</td>
<td>Sending Records Administrator</td>
<td>Enter the name of the records administrator for the Division or Office here. The records administrator for the sending office signs or initials here.</td>
</tr>
<tr>
<td>4</td>
<td>Sending Records Coordinator</td>
<td>Enter the name of the records coordinator (the person completing the form and sending the records) for the sending office here.</td>
</tr>
</tbody>
</table>
### How To Complete Form 1419

<table>
<thead>
<tr>
<th>Step</th>
<th>Block Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Date</td>
<td>Enter date of shipment.</td>
</tr>
<tr>
<td>6</td>
<td>Request the accompanying records be...</td>
<td>Check one box to indicate disposition or handling instructions.</td>
</tr>
<tr>
<td>7</td>
<td>Remarks</td>
<td>Enter notes or special instructions, such as whether the records being transferred are vital records, or records subject to state archives review requirements, etc.</td>
</tr>
<tr>
<td>8</td>
<td>Storage Location</td>
<td>Leave blank. Completed by recipient storing the records.</td>
</tr>
<tr>
<td>9</td>
<td>Box No.</td>
<td>List each box number (i.e., 1, 2, etc.).</td>
</tr>
<tr>
<td>10</td>
<td>Record Series Title</td>
<td><strong>For each box, enter the record series title from the TxDOT records retention schedule.</strong> Since these titles are broad and may include several types of records, select the part of the title that most accurately describes the records. You do not have to copy the entire title. Abbreviate, if necessary. (Remember, each box shall contain only one record series.</td>
</tr>
<tr>
<td>11</td>
<td>Agency Item No.</td>
<td>For each record series, enter the agency item number from the TxDOT records retention schedule. This entry is required for records sent for storage at Records management or the State Records Center, or for coordination of archival review. <strong>NOTE:</strong> For record series common to all TxDOT offices, add your office's functional account number to the agency item number. For example, if the agency item number for a common records series is ADM09 and the records belong to a unit whose functional account number is 18, enter 18ADM09.</td>
</tr>
<tr>
<td>12</td>
<td>Description &amp; Date of Records</td>
<td>Enter information sufficiently specific to identify the records in each box for your retrieval purposes. Always include the date of the records. It may be enough to list only beginning and ending file names, dates, number sequences or other identification sufficient to identify box contents. If a more detailed description is needed or there is not enough room on Form 1419, attach a separate listing or index to the transmittal form. Records being sent for State Archives review need only beginning and ending file names, dates, number sequences or other identification sufficient to identify the contents of each box.</td>
</tr>
</tbody>
</table>
When the form is complete and you are ready to send the records, retain a copy for your pending file and place the original under the lid of box number 1 of your shipment.

In Austin, shipments of five or fewer boxes may be sent through interoffice mail. For larger amounts, call 512-465-7390 to arrange shipment.

### How To Complete Form 1419

<table>
<thead>
<tr>
<th>Step</th>
<th>Block Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Destruction Date (Year)</td>
<td>Enter the date records are to be destroyed in accordance with the TxDOT Records Retention Schedule. Use this format: MM/YY. Calculate the destruction date based on the code in the Total Retention Period block on the TxDOT Records Retention Schedule. If the code is FE+3 (end of fiscal year plus three years) enter 09/ and the third fiscal year after the end of the fiscal year of the records.</td>
</tr>
</tbody>
</table>
Section 4 — Receipt and Storage Location

Receipt Procedures

On receipt of records transferred to storage, records management does the following:

- Verifies that the records are eligible for storage at a records center. Records management checks the enclosed Form 1419, Records Transmittal, against the TxDOT records retention schedule. Records will be returned to the sender if:
  - Form 1419 is missing, incomplete, inaccurate or illegible,
  - records transferred are not record copies,
  - records are not packed in standard document storage boxes.

- Verifies that the beginning and ending records in each box correspond with the information on Form 1419.

- Assigns storage and returns a copy of the transmittal with the storage locations entered.
Section 5 — Retrieving Records

Procedure

To retrieve records from storage, contact records management and request the records by referring to the 4-digit storage location number on your copy of the records transmittal (Form 1419).

You may request the entire box or a specific folder.

Monitoring of Checked-Out Records

When you request records from storage, records management will obtain your name, office and phone number for a checkout file.

Every six months, records management contacts employees who have checked out records to verify that the records are still in the possession of that person, and to encourage the return of the records to storage if they are no longer needed.

When you are finished with the records, simply return them to records management via interoffice mail.
Section 6 — Storage Areas and Equipment

Introduction

For districts and any offices maintaining an inactive records storage area, this section contains information on

- storage area requirements,
- box identification, and
- types of storage boxes available.

Essential Requirements for Storage Areas

- Make sure storage areas are secure. Provide protection from:
  - the elements: A windowless, air-conditioned environment is best;
  - insects: Food and drink should not be allowed in the storage area;
  - fire: A storage area with a fire-suppression sprinkler system is ideal. Suitable fire extinguishers should be accessible. Smoking in or near the storage area should be strictly prohibited. Do not store volatile substances in or near the same place as records;
  - access by unauthorized people.

- Use shelving. Metal shelves are best. Keep the bottom shelf at least two or three inches off the floor. For fast retrieval, you may organize the shelving area by record types, fiscal years, etc. Use shelf labels.

- Stack boxes. If shelving is not practical or available, stack boxes on pallets or some other support that keeps them off the floor. Cardboard document storage boxes may be stacked up to six high. It helps to insert 1/4-inch plywood between boxes. Cut plywood sheets a little larger than the lids of the boxes. Attach a large label identifying the stacked records to a box on the outside of the stack, or even individual outside boxes. Retrieval is more difficult with this storage method.

Record Location Aids

Index stored

records in sufficient detail to retrieve them. Form 1419 is designed to capture this information. Include the location (pallet number, shelf location, etc.), a reference to the Agency Item Number on the TxDOT records retention schedule, and the date the records become eligible for destruction on the index. Furnish a copy of the index in a pending file, arranged by destruction date, to your
records administrator. The list can serve as a detail attachment when documenting records destruction.

For quick retrieval, attach an index or list of contents to each box. Avoid adhesives that attract insects. You may also want to place a copy of the index inside the box.

Mark boxes visibly to identify the contents and destruction date. Include only records with the same destruction date in any single box. Use different colored markers for different destruction dates, and avoid colors that fade in sunlight. Mark any boxes that contain either vital records or records requiring review by the State Archives before destruction.

Types of Storage Boxes

Although the standard document storage box is the only type allowed at the TxDOT records center or State Records Center, there are occasions when other types of boxes may be needed for local use. The table below describes several types of storage boxes.

<table>
<thead>
<tr>
<th>Box Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Document Storage Box</td>
<td>Standard document storage boxes are one cubic foot in volume, measuring 10 x 12 x 15 inches. They hold letter- and legal-size documents and have removable lids. Empty boxes fold flat for storage. Request these boxes from local supply rooms, Regional Distribution Centers or warehouses (NIGP # 615-37-13-0850).</td>
</tr>
</tbody>
</table>
| Permafile Box                   | These boxes are also known as transfer boxes. The standard size is 10 x 12 x 24 inches, and the legal size is 10 x 15 x 24 inches. The boxes are collapsible and reusable. Each has the same volume as a file drawer. Permafile boxes are commercially available. While useful for storing some types of records such as rolled maps or large documents, Permafile boxes have some disadvantages:  
  • Weight: a full box weighs up to 100 pounds.  
  • Hazards: the metal reinforcing strip can cut hands and rip clothing.  
  • Inefficient use of space: Boxes cannot be stacked more than four or five high without crushing the box on the bottom. Legal-size boxes do not fit standard shelving. |
| Bankers Box                     | These cardboard boxes slip into metal-reinforced cardboard shelving units. They are the same size as standard document storage boxes. Bankers' boxes are an inexpensive way to store records. However, the shelving units will not support more than seven or eight full boxes in a stack, and you must dismantle an entire stack to replace a worn unit. The units tend to weaken with time and use, and may become dangerously unstable. |
| Custom Box                      | Some offices make wooden boxes to store construction project records. Each project has its own box, which simplifies moves and transfers.                                                                                                                                  |
| Other                           | Cardboard boxes for use with specific media are available under state contract (commodity code 640-25-60).                                                                                                                                   |
Chapter 9 — Microfilming Records

Contents:

Section 1 — Overview
Section 2 — Procedural Outline
Section 3 — Microfilm Storage, Equipment and Maintenance
Chapter 9 — Microfilming Records

Section 1 — Overview

Introduction and General Guidelines

Sections 441.188 and 441.189 of the Government Code authorize agencies to retain records on microfilm or electronically. Document imaging involves the conversion of hard copy original documents or records to an alternative medium. Records with permanent or long term (more than 20 years) retention periods or archival requirements may be retained on microfilm. Offices choosing to microfilm records may obtain those services through a purchase of services. This chapter contains guidelines for microfilming. See Chapter 5, “Electronic Records,” for information on electronic imaging.

Storing, Scanning or Microfilming?

The majority of department records require retention for fewer than five years. For all but permanent or archival records, storage in the original format is the easiest and cheapest way to retain hard copy inactive records until their destruction date.

Scanning records to an electronic system has replaced microfilming of hard copy files that require lengthy retention as a standard department practice. Scanning is most efficient when done at the time a record would ordinarily be filed. Batch scanning of files for electronic storage is almost as labor-intensive as microfilming.

The space-saving and distribution advantages of microfilm can be achieved by electronic imaging without incurring the limitations of film. Microfilming is labor-intensive and expensive. Managers should carefully evaluate the actual need to use microfilm. Considerations include the manpower to prepare and index the records for microfilming, to inspect the microfilm product after filming and
the cost, availability and maintenance of equipment to store and read or print copies from the microfilm. The following table describes the advantages and limitations of microfilm.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ <strong>Space savings.</strong> Microfilm concentrates a large volume of information in a small package. One 250-foot roll of 16 mm microfilm can hold the equivalent of a document storage box of records (up to 4,200 8-1/2-by-11-inch pages or images). Nine 100-foot rolls can store the equivalent of one five-drawer file cabinet (25,000 8-1/2-by-11-inch pages or images).</td>
<td>✓ <strong>Expense.</strong> Microfilm is expensive and labor intensive to create.</td>
</tr>
<tr>
<td>✓ <strong>Low cost distribution.</strong> Microfilm is inexpensive to duplicate.</td>
<td>✓ <strong>Unclear copy.</strong> The quality of the original record affects the quality of the filmed image. Old, faded or damaged documents may not reproduce clearly. Colors do not appear, and it may be difficult to tell whether a filmed record is the original. Official certifications and explanatory notes filmed with the records on target sheets can address these limitations to some extent.</td>
</tr>
<tr>
<td>✓ <strong>File integrity.</strong> Once filmed, all records in a file are together, and individual records cannot be physically removed, lost or misfiled. Any alterations are apparent.</td>
<td>✓ <strong>Equipment requirements.</strong> Microfilm requires equipment ranging from simple readers that cost as little as $150 to highly advanced reader/printers that can cost up to $30,000. Continuing availability of equipment and service support over time may present difficulties in using microfilm for archival preservation.</td>
</tr>
<tr>
<td>✓ <strong>Security.</strong> Duplicate security copies can be stored in a separate place</td>
<td>✓ <strong>Environmental storage considerations.</strong> Microfilm will deteriorate if it is stored in an environment that does not have temperature and humidity controls. See &quot;Storage Environment&quot; in this chapter. The product of deterioration, acetic acid, may present a workplace hazard to employees.</td>
</tr>
<tr>
<td>✓ <strong>Archival preservation.</strong> Microfilm may be used for reference in place of original documents and can offer an increased life span.</td>
<td>✓ <strong>User resistance.</strong> Using microfilm and microfilm equipment for any length of time can be tedious.</td>
</tr>
<tr>
<td>✓ <strong>Convertability.</strong> Microfilm images may be converted to paper or, with proper equipment, digitized.</td>
<td></td>
</tr>
</tbody>
</table>

**Microfilm Formats**

The most commonly used microfilm formats include:

**Roll film:** The most economical microform, 16 mm width is typically used for documents, and 35 mm widths are used for larger format documents such as drawings or maps. Roll film ensures file integrity and is best used for long-term storage of inactive records.

**Microfiche:** A sheet of 105mm film (usually 4 inches by 6 inches) that can contain at least 98 images (depending on the size of the originals), microfiche is best used for frequently referenced files. An eye-readable label makes retrieval easier. Because a microfiche is a single unit, it provides reasonable file integrity. It is moderately expensive to produce, although a microfiche reader is the
least expensive type of microfilm reader. Microfiche, jackets (transparent cards 4 inches by 6 inches with chambers for the insertion of individual frames or strips of microfilm) are typically produced and the customer is furnished a microfiche duplicate for active use.

Microfiche, jackets (transparent cards 4 inches by 6 inches with chambers for the insertion of individual frames or strips of microfilm) are typically produced and the customer is furnished a microfiche duplicate for active use.
Section 2 — Procedural Outline

The following table describes the procedures involved in a typical microfilming project. Depending on the details of the service purchase, individual steps may be performed by either the customer or the vendor.

<table>
<thead>
<tr>
<th>Step</th>
<th>Responsible</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Customer and Vendor</td>
<td>Develop specifications for the film job, to include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Film type (roll film or microfiche)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Reduction ratio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Orientation of documents on film</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Indexing and electronic image count (blip) marking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Density or resolution requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Number of duplicate (backup) copies</td>
</tr>
<tr>
<td>2</td>
<td>Customer or Vendor (according to service agreement)</td>
<td>Prepares records for filming by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ removing fasteners, buck slips and unnecessary documents, repairing torn pages, taping small documents to letter-sized sheets and photocopying photographs on a copier capable of producing a usable image;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ preparing targets to certify record authenticity, identify the job/file and specific files or folders and places them in front of the folders;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ preparing a detailed index of folders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ boxing and shipping records to the vendor.</td>
</tr>
<tr>
<td>3</td>
<td>Vendor</td>
<td>◆ films the records and enters the blip (frame) count on the index, which is then filmed and spliced onto the beginning of the roll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ sends the film product to Records management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ retains the records in case any documents need to be re-filmed</td>
</tr>
<tr>
<td>4</td>
<td>Customer</td>
<td>◆ inspects the microfilm and advises vendor of acceptance of the microfilm or corrections needed, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ arranges disposition of the hard copy originals.</td>
</tr>
<tr>
<td>5</td>
<td>Service Bureau</td>
<td>◆ Films the records and enters the blip (frame) count on the index, which is then filmed and spliced onto the beginning of the roll.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Sends the film product to Records management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Retains the records in case any documents need to be re-filmed.</td>
</tr>
</tbody>
</table>

Microfilm Job Specifications

Microfilm job specifications direct the vendor on job requirements and should include information describing

◆ record series;
◆ microfilm format (roll film, microfiche or other microform);
Records Management

Chapter 9 — Microfilming Records

Section 2 — Procedural Outline

● reduction ratio (size of the microfilmed image), which is related to the user's microfilm reading equipment;

● orientation (arrangement of images on the film);

● filming cycles (if appropriate for frequently scheduled jobs);

● distribution of microfilm original copies; and

● special filming, indexing or handling instructions.

Preparing Records for Microfilming

Documents are normally filmed on an automatic camera that works like a high-speed copier. Remove any fasteners and use transparent tape to repair tears that will jam the camera. Tape small documents to an 8½ x 11- inch sheet of paper and make photocopies of photographs on a copier with a setting that will produce a usable image.

Purge and Organize: Remove all duplicate copies and unnecessary materials. If there is a choice between original documents, carbons or photocopies use the original documents to ensure optimal image quality. Arrange all folders in the sequence in which they are to be filmed.

Prepare an index of the records. List each folder or subdivision of records to be microfilmed in its proper order. It is convenient to create and insert target sheets while indexing the records. Click here to obtain an index sheet in Word.

Target sheets are 8 ½ x 11- inch pages that are based on the index and microfilmed with records to visually identify separate files or records. They serve a purpose on film similar to that served by file guides and folder labels in a file cabinet. Click here to obtain a sample target sheet.

In the case of oversized documents, cut them into a size consistent with the surrounding documents, prepare a target with a drawing showing all of the parts. An example target is illustrated below. Label each part (A, B, C, D, etc.) filmed as a separate image. This will show users how the parts fit into a whole document.
Records Certification

Certification sheets attest that the filmed images are true and correct reproductions of the original records and should be signed by the person performing the filming and inserted in to the beginning of the film roll or the first image on a fiche.

Distribution of Microfilm

Typically microfilm jobs specify production of an original and a duplicate. Use the duplicate for any reference purposes, and store the original in a separate location as a security backup.

Disposition of Original Records

The customer may arrange for the vendor to destroy the original records on acceptance of the microfilm job, or may choose to have the originals returned and to manage the destruction internally. The destruction does not have to be documented on the Form 1420, Records Destruction Log, since the records themselves still exist, and only the medium containing them has changed.

Reviewing Microfilm for Deterioration

Microfilmed records must be retained and maintained in compliance with Government Code, Chapter 441, and the state Microfilming Standards and Procedures (13 TAC §§6.21 -- 6.35). Offices maintaining microfilmed records must conduct an ongoing review of microfilm for signs of deterioration. Contact records management to arrange duplication of film showing signs of deterioration to new film stock.
Section 3 — Microfilm Storage, Equipment and Maintenance

Storage Environment

Microfilmed records with a retention period exceeding ten years must be stored in a temperature that does not exceed 70°F Fahrenheit, and a constant relative humidity of 35% must be maintained with a maximum variance of +/- 5.0% relative humidity in a 24 hour period.

Microfilmed records with a retention period of less than ten years must be kept in an environment where the maximum temperature does not exceed 77°F Fahrenheit, and the relative humidity is maintained in a range between 20% and 50%, with a maximum variation of +/- 5.0% relative humidity in a 24 hour period.

A typical air-conditioned office environment with stable temperature and humidity where microfilm will have minimum exposure to light and contaminants, is generally adequate for film to be retained for ten years or less.

Microfilm Equipment

Offices that keep microfilmed records need a means of reading the microfilm. The two basic types of microfilm equipment are:

- **Readers.** Readers are only for viewing microfilm, microfiche or other microforms. The least expensive readers are for microfiche. More expensive readers have interchangeable carriages for viewing different microforms. Readers may have various other features, including motorized carriages for high-speed searching and retrieval, and/or digital displays for frame counters.

- **Reader/printers.** Reader/printers combine a reader with the capability to produce a paper copy of the image that is on the screen. They may be purchased with the same options described above.

**NOTE:** Although simple reader/printers are available on state contract, you may require specific features that necessitate an open market purchase. Depending on their features, reader/printers can cost up to $50,000.

Microfilm equipment is available under state contract and the following commodity codes:

- microfiche readers: 575-72-05, 10
- microfiche reader/printers: 575-76-00
- microfilm readers: 575-72-50, 55
Selecting Equipment

In addition to cost, consider these factors in selecting microfilm equipment:

**Screen size.** The reader screen should display an entire page of information at or near the original size of the record. The screen image will be the same size as the original record if the magnification of the lens on the reader equals the reduction ratio of the microfilm. (The reduction ratio is the amount a record is reduced on film. For example, a reduction ratio of 24:1 means a record is reduced to 1/24 of its original size.) An 8½ by11-inch record filmed at a reduction ratio of 24:1 will be the same size as the original when viewed on a reader with a 24X lens.

A screen smaller than the original record will display a full page from the original if the magnification of the lens on the reader is **less** than the reduction ratio of the microfilm. An 8½ by 11-inch record filmed at a reduction ratio of 24:1 can be viewed in its entirety on a 7¼ by 9½-inch screen if the reader has 20X magnification. The entire image will be proportionately smaller than the original.

**NOTE:** A reader with a lens magnification **greater** than the reduction ratio of the microfilm will **not** display a full page from the original record unless the screen is proportionately larger.

- **Screen color.** Neutral viewing screens are standard. They are available in tints of blue, green and gray. Tinted screens reduce eyestrain, particularly in high-use situations.

- **Screen type.** Most readers and reader/printers are the rear-projection type. They project the image from the rear of the unit onto the back of a translucent screen. Some of these screens are reversible. One side has a matte finish to reduce glare and reflections, and the other has a shiny surface for sharper images.

- **Unit size.** The size of microfilm equipment varies. Small, portable readers fold into a traveling case. Desktop equipment is larger in size and most common. Larger freestanding units have many features, functions and controls. Prices vary according to size and features.

- **Optics.** Readers and reader/printers are specified by image magnification. For example, 24X means that the image is magnified 24 times. Lower-priced equipment has a fixed magnification. When selecting equipment for viewing different microforms, make sure the magnification of the equipment or lens is compatible with the reduction ratios of the microforms to be viewed. Equipment capable of handling a variety of microforms usually provides variable magnification through one of the following methods:
  - interchangeable lenses
  - dual lenses controlled by a lever or other mechanism
  - zoom lenses.

- **Special features.** A device called a blip-chip is helpful on readers that have a motorized carriage and are used in high-retrieval situations. Electronic frame counters, or blips, are inserted
on roll film as it is shot. The blip-chip reads the blips and displays the frame numbers as the motorized carriage goes through the film. When the desired frame number is displayed, the user can stop the film. (Frame numbers are identified in the index at the beginning of the film.) Most mid-priced to high-priced equipment with motorized carriages comes with a digital display already installed.

**Maintenance of Equipment**

The quality of a microfilmed image, or a paper copy produced from the image, depends on the cleanliness of the optical system and printing mechanism.

Dust on screens, mirrors or lenses reduces light and clarity. Dust particles can damage film and impair readability.

Prolong the life of microfilm equipment as follows:

- Use a dust cover when the equipment is not in use.
- Clean screens and optical systems routinely, following the manufacturer's recommendations.
- Take care in loading paper, chemicals, and toner into reader/printers.
- When a bulb begins to darken, replace it.
- **Never touch halogen bulbs.** They burn extremely hot and can ignite any residue of oil from human skin.
- Inspect and clean equipment routinely. A small, handheld vacuum cleaner with a long, thin nozzle works well.

**Integrating Microfilm and Emerging Technologies**

With the proper equipment, microfilm images may be scanned to digital images. Large backfile conversions of microfilmed records to digital images are generally not practical unless the records are subject to a high rate of retrieval and reproduction or the scanning is necessary to arrest deteriorating images. Large scale imaging projects are best handled by using a vendor who specializes in them. Microfilmed records converted to digital are subject to the requirements for electronic records described in Chapter 5, Electronic Records.
Chapter 10 — Records Destruction

Contents:

Section 1 — Overview
Section 2 — Destruction Procedures
Section 3 — Records Destruction Log
Section 4 — Confidential Records
Section 5 — Archival Review
Section 1 — Overview

Authorization for Destruction

Texas Government Code §441.187 authorizes TxDOT to dispose of any record listed on the approved TxDOT records retention schedule once the required retention period has been met.

NOTE: Records involved in an audit, investigation, litigation or open records request cannot be destroyed until conclusion of the action involving those records.

Advantages of Timely Disposal

Destroying records as soon as they become eligible after having met their retention requirement benefits the department by:

- reducing exposure to legal discovery and open records demands. There is no requirement to produce records that were destroyed in the normal course of business, as long as there was no anticipated or actual legal action in place at the time of their destruction that would have required us to withhold them from destruction, and

- reducing the cost of storage (physical space and equipment, virtual space, system performance), since the department now pays an external vendor for server storage and network bandwidth services. Benefit will also accrue as enterprise FileNet libraries accumulate content over time.

Records Eligible for Destruction

Official (record copy) records are eligible for destruction when they have been retained for the total retention period in the TxDOT records retention schedule.

Non-record convenience or information copies and e-mail of a transitory nature may be destroyed without formality once their purpose has been served.

Withholding Records from Destruction

Records involved in an audit, investigation, litigation or an open records request shall not become eligible for destruction until the final conclusion of the action and satisfaction of the retention requirements pertaining to records related to the action.

Take steps to identify and preserve records involved in such actions as soon as you become aware of the possibility of the action, and include steps to verify conclusion of any actions during review.
of eligibility for destruction. Coordinate with the Office of General Counsel (OGC) to determine the status of any records subject to a litigation hold before authorizing their destruction.
Section 2 — Destruction Procedures

Destruction of Records Retained Locally

Districts, divisions or offices (D/D/Os) may destroy records retained locally once the total retention period has been met. The responsible office must document the destruction of official state records on Form 1420, Records Destruction Log, available in e-Forms on Crossroads, and forward the log through the records administrator to TxDOT records management.

TxDOT Records Management sends broadcast emails to DDO Records Administrators shortly after the turn of the fiscal and calendar year as a reminder to review retained records and identify those that are eligible for destruction. Records Administrators shall forward these reminders to all offices and work units in their organization. Establishing a suspense date and pointing recipients to Form 1420 in e-Forms is good practice.

Local Review and Approval Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Who</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Records Custodian</td>
<td>Uses file plan to review and identify records that have met their retention and that are eligible for destruction and list them on the Form 1420. (Custodians may delegate this task to Records Coordinators, but the Custodian is required to approve destruction).</td>
</tr>
<tr>
<td>2.</td>
<td>Records Custodian</td>
<td>Forwards Form 1420 to DDO Records Administrator.</td>
</tr>
<tr>
<td>3.</td>
<td>Records Administrator</td>
<td>Verifies that the records listed on the form have met their minimum required retention period to approve the destruction. If the destruction is disapproved, the Records Administrator must describe the reason to the Custodian. Returns the Form 1420 to Custodian.</td>
</tr>
<tr>
<td>4.</td>
<td>Records Custodian</td>
<td>Enters their authorization and the date on the Form 1420 and proceeds with the destruction/deletion of records. On completion of the destruction, forwards the Form 1420 to the Records Administrator.</td>
</tr>
<tr>
<td>5.</td>
<td>Records Administrator</td>
<td>Forwards Form 1420 as an email attachment to TxDOT Records Management.</td>
</tr>
<tr>
<td>6.</td>
<td>TxDOT Records Management</td>
<td>Files the Forms 1420 in the agency's Records Destruction Log file to retain for ten years.</td>
</tr>
</tbody>
</table>

Destruction of Stored Headquarters Division and Office Records

For division or office records stored at the TxDOT records center, the TxDOT records manager advises the records administrator of the scheduled destruction date of eligible records by e-mail.
with images of the original transmittals for the records attached as a detail reference. The records administrator receiving the e-mail coordinates local approval with the records coordinators who sent the records for storage.

The destruction coordination message includes a suspense date by which the office responsible for the records must respond to withhold the destruction of any particular records and a request for an explanation of the withholding to inform any future person responsible for the records during subsequent reviews for destruction.

No response within the suspense date means that the division or office certifies that all retention requirements have been met, and authorizes destruction of the records in accordance with the approved TxDOT records retention schedule.

**Extended Retention**

If it is necessary to retain stored records for an additional period, you must contact records management by the suspense date in the records destruction coordination memo. Records management will need the reason for postponing destruction and an estimated destruction date.

This contact may be by telephone, memorandum, e-mail or even by a handwritten note on the destruction coordination memo itself. It is important that records management have documentation on file to support any extended retention request.

Records management will retain the records and will include them in future destruction coordination communications to monitor their status. The responsible office can request their destruction at any time.

**Electronic Records Destruction**

Record "deletion" merely removes the index marker from the disk; the record remains to be written over, much like recording over an old audio or video tape. Eventually the record may disappear through fragmentation and overwrites; however, the possibility of forensic reconstruction exists.

Full deletion of obsolete records involves drive formatting and recopying to ensure complete removal, which is generally impractical in an enterprise environment. A possible solution involves retaining selected high-risk records on a server dedicated to managing volatile records through a combination of file deletion, copying, disk formatting and reloading procedures.

FileNet EDMS eliminates these risks, as deletions actually destroy documents and records, completely eliminating them from the system.
Overview of Records Destruction in EDMS

Chapter 4, Section 3, discusses specific procedures for managing records in the EDMS, and includes the system management steps involved in records destruction.

During periodic file management activities, searches based on combinations of document properties such as record type, status and date are run to retrieve and report to the OPR records in the EDMS that have met their retention and that are eligible for destruction. The OPR then authorizes destruction or identifies any documents or records to be retained further. Once developed, the searches can be saved to be run again at the next interval with only a revision of the date value.

On approval to destroy, the system administrator creates a report of the documents/records to be destroyed for the OPR to attach to the Form 1420 and deletes the documents/records from the EDMS. Depending on local practice, the OPR forwards the 1420 to its DDO records administrator or directly to SSD records management.
Section 3 — Records Destruction Log

Logging Destruction

13 TAC §6.8(b)(3) requires that the destruction of state records be documented. TxDOT Form 1420, Records Destruction Log, is available in the SSD folder of the EForms site on Crossroads.

DDO records administrators must log records destroyed locally by their organizations. As individual records coordinators complete the logs, the records administrator can compile them into a single records destruction log for the organization to submit to the TxDOT Records Management Officer.

Destruction logs may be submitted to records management in a batch mode once a year, or as individual offices complete them. The preferred method is to attach them as PDF files to an e-mail to the records management officer. Records management maintains the official disposition log for the entire department.

Records management maintains the TxDOT records destruction log on a fiscal year basis. D/D/O logs forwarded to records management will be filed according to the fiscal year during which the records are destroyed and retain for the 10-year requirement in the State of Texas Records Retention Schedule.

Information on the Log

The following figure illustrates a completed Form 1420.
## Records Destruction Log

### Chapter 10 — Records Destruction

### Section 3 — Records Destruction Log

<table>
<thead>
<tr>
<th>Agency Item Number</th>
<th>Description and Date of Records</th>
<th>Total Retention</th>
<th>Date Destroyed</th>
<th>Destruction Authorized By</th>
</tr>
</thead>
<tbody>
<tr>
<td>4A4DC01</td>
<td>File Plan FY 2005 and prior</td>
<td>US</td>
<td>1/29/06</td>
<td>T. MacMommom</td>
</tr>
<tr>
<td>4A4DM08</td>
<td>Monthly Production Reports prior to 09-01-07</td>
<td>AV+1</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC01</td>
<td>Budget request and monitoring FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC04</td>
<td>Material requests, purchasing files FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC07</td>
<td>Office inventory records FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC08</td>
<td>Public information activity reports FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC10</td>
<td>Interagency and Intercollaboration agreements, and records FY 2004</td>
<td>AC+1</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC11</td>
<td>Charge cards, FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC19</td>
<td>Charges for copies made, copies of transmittals FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4AC23</td>
<td>Charge schedules, copy price list documentation FY 2005 and prior</td>
<td>US+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4DM02</td>
<td>General correspondence FY 2007 and prior</td>
<td>AV+1</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4DC13</td>
<td>Work orders, reproduction requests FY 2007</td>
<td>AV+1</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4DN00</td>
<td>Public Info requests, certifications, etc. FY 2000</td>
<td>AC+2</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4DM17</td>
<td>Internal procedures superseded through FY 2007</td>
<td>US+1</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4ER16</td>
<td>Employee ILS requests FY 2005</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4M002</td>
<td>Agency Records Destruction Files FY 1999 and prior</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
<tr>
<td>4A4M001</td>
<td>Microfilm acceptance, Hard copy destruction authorization FY 2005 and prior</td>
<td>FE+3</td>
<td>1/29/06</td>
<td>*</td>
</tr>
</tbody>
</table>

### Instructions and Example

- **Instructions and Example (Delete when no longer needed):**
  - Identify DDO and specific section or office by using functional account numbers with the Agency Item Number citation from the TxDOT Records Retention Schedule. Record description may be general, but must be adequate to identify the record series. Detailed indexes or listings of records may be attached, if available, but are not required. Contact GSD Records Management before destroying any record series that has an archival review requirement in the TxDOT Records Retention Schedule (Archive column = "A" or "R.")
  - FORWARD: Completed log form to GSD Records Management (May be sent as hard copy or as email attachment).

---

*Records Management 10-8*  
*TxDOT 12/2014*
The records destruction log includes the following information about records that are destroyed:

- Citation to the Agency Item Number of the records on the TxDOT records retention schedule
- Sufficient description of the records destroyed, including:
  - record series title,
  - date of records,
  - quantity/volume of records,
  - additional information such as detail listing of file contents, indexes or other descriptive material may be attached to the log.
- Total retention requirement
- Date of destruction
- Name of records administrator (or a designee) authorizing destruction of records and certifying that retention requirements, such as applicable audits, etc., have been met.
Section 4 — Confidential Records

Destruction of Confidential Records

Shredding is the method of destruction to be used for all confidential records.

Follow these procedures to shred confidential records in any medium:

◆ **Districts:**
  - Use private shredding facilities, or shred records on-site.
  - If records are to be recycled after shredding, make sure that recycling contractors certify confidentiality from pickup through ultimate disposition.
  - The district records administrator (or records coordinator) certifies on the district's disposition log that the records have been shredded.

◆ **Austin headquarters divisions and offices:**
  - Send records to records management for handling. Records management arranges shredding services with a vendor.

If no shredder is available and the quantity of records is small, dispose of confidential records in the following way:

◆ Cut or tear records by hand into small pieces.
◆ Mix pieces thoroughly, and place them in several different containers with other trash.
◆ Discard containers separately at varying intervals.

Destruction of Non-Confidential Records

Recycling is the preferred method of destruction for non-confidential records. Non-confidential records do not need to be shredded before recycling. Other methods of destroying non-confidential records are:

◆ pulping or burning
◆ general disposal (commercial trash removal, bulk disposal, use of local landfills)
◆ erasure or re-recording over magnetic media, audio or video media.

NOTE: Methods other than burning records and depositing them in landfills are preferable.
Section 5 — Archival Review

Archival Records

Texas Government Code §441.186 requires that certain records series, identified on the TxDOT records retention schedule with an archival code "R," be reviewed by the State Archives—once they have met their retention in the agency—to determine whether the records may have sufficient historical value to be retained by the State Archives. Other records, identified with an archival code "A," must be sent to the State Archives.

The following table lists records that are subject to archival review. An asterisk (*) indicates that archival review requirements are frequently satisfied by the deposit of copies of published documents with the State Publications Clearinghouse.

<table>
<thead>
<tr>
<th>Record Series (Records and documentation related to….)</th>
<th>Arch. Code</th>
<th>Agency RRS Item #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative correspondence (Executive staff, board or commission members, DDs, DEs and program heads)</td>
<td>R</td>
<td>ADM01</td>
</tr>
<tr>
<td>Agency rules, policies, procedures, including manuals and working files</td>
<td>R*</td>
<td>ADM27&amp;28 54ACV01</td>
</tr>
<tr>
<td>Annual financial report</td>
<td>A*</td>
<td>43ACM07</td>
</tr>
<tr>
<td>Biennial narrative reports to the Governor</td>
<td>A*</td>
<td>ADM17</td>
</tr>
<tr>
<td>Calendars, appointment books, scheduling or itineraries (Executive staff, board or commission members, DDs, DEs and program heads)</td>
<td>R</td>
<td>ADM47</td>
</tr>
<tr>
<td>Commission agendas and minutes</td>
<td>A*</td>
<td>41AEO02 42 AD101 79OGC04</td>
</tr>
<tr>
<td>Commission meeting supporting documentation</td>
<td>A</td>
<td>41AEO08</td>
</tr>
<tr>
<td>Executive orders (Documents that initiate, rescind or amend regulations, policies or procedures governing programs, services or projects of an agency)</td>
<td>A</td>
<td>ADM03</td>
</tr>
<tr>
<td>History files</td>
<td>R</td>
<td>ADM25</td>
</tr>
<tr>
<td>Legislative appropriation requests</td>
<td>A*</td>
<td>43FBF01</td>
</tr>
<tr>
<td>Non-fiscal reports and studies compiled by agency personnel or external consultants</td>
<td>R*</td>
<td>ADM15 70RTI01</td>
</tr>
<tr>
<td>Organization charts, originals</td>
<td>A</td>
<td>ADM24</td>
</tr>
<tr>
<td>Plans (not construction) plans and planning records</td>
<td>R</td>
<td>ADM12</td>
</tr>
</tbody>
</table>
### Chapter 10 — Records Destruction

#### Section 5 — Archival Review

<table>
<thead>
<tr>
<th>Record Series (Records and documentation related to...)</th>
<th>Arch. Code</th>
<th>Agency RRS Item #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public relations</td>
<td>R*</td>
<td>ADM21 75GPM01&amp;02</td>
</tr>
<tr>
<td>Publication development files (does not apply to drafts</td>
<td>R</td>
<td>ADM19</td>
</tr>
<tr>
<td>of text, production paste-ups or production materials for</td>
<td></td>
<td></td>
</tr>
<tr>
<td>routinely distributed publications or brochures)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speeches, papers or presentations (including notes and/or</td>
<td>R</td>
<td>ADM22</td>
</tr>
<tr>
<td>text) delivered in conjunction with agency work</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic highway research program</td>
<td>R</td>
<td>46PAV03</td>
</tr>
<tr>
<td>Strategic plans</td>
<td>A*</td>
<td>41DED01 75GPM04</td>
</tr>
<tr>
<td><strong>Legal and Legislative Records</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative hearings</td>
<td>R</td>
<td>ADM34</td>
</tr>
<tr>
<td>Legal case files</td>
<td>R</td>
<td>ADM33 60TOR03 79O</td>
</tr>
<tr>
<td>Legal opinions and advice</td>
<td>R</td>
<td>42AD102 79O</td>
</tr>
<tr>
<td>Sunset Review</td>
<td>R</td>
<td>ADM32 75GPA01</td>
</tr>
<tr>
<td><strong>Facilities and Transportation Planning/Operations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architectural building construction project contracts,</td>
<td>R</td>
<td>DECO02&amp;03 44SSV</td>
</tr>
<tr>
<td>files, plans and specifications</td>
<td></td>
<td>46CCP02 47FMS01 &amp; 02, 04</td>
</tr>
<tr>
<td>District buildings</td>
<td>R</td>
<td>DMT03</td>
</tr>
<tr>
<td>Cultural resources photographic negatives</td>
<td>A</td>
<td>57CRM02</td>
</tr>
<tr>
<td>International bridge crossings</td>
<td>R</td>
<td>50TSP08</td>
</tr>
<tr>
<td>Metropolitan/Rural Transportation Plan</td>
<td>R*</td>
<td>TPD03 50TSP02</td>
</tr>
<tr>
<td>Quarry and pit files</td>
<td>R</td>
<td>47MNT05</td>
</tr>
<tr>
<td>Railroad company annual reports</td>
<td>A</td>
<td>83</td>
</tr>
<tr>
<td>Statewide transportation plan</td>
<td>R</td>
<td>50TSP01</td>
</tr>
</tbody>
</table>
Chapter 10 — Records Destruction

Section 5 — Archival Review

Identifying Archival Records

The best time to identify records with archival requirements is when listing them on a file plan. Identify records requiring archival review in the remarks block on Form 1419, and on any index documentation when preparing records for storage.

When referencing the TxDOT records retention schedule to complete the Records Destruction Log prior to actual destruction of records, check again to make sure there is no archival requirement for the records series.

Handling Archival Records

The archival requirement for some records is met when required copies are sent to the State Library Publications Depository Program. Records management has annotated the TxDOT records retention schedule to indicate that an archival copy of eligible documents be furnished to records management for archival deposit at the time the documents are produced. This step applies particularly to records that are not necessarily "published," and is intended to satisfy the archival requirement without the producing office having to perform extra steps at the end of the record/document's life cycle.

Records management coordinates archival review for applicable records with the State Archives. Districts, divisions and offices processing records with an archival requirement at the end of their retention must prepare a Form 1419, “Records Transmittal,” pack the records in a suitable unmarked document box and ship the records to Records Management for further coordination with the state archives.

Archival Records in an EDMS

The State Archives is not capable of accepting electronic records for review or archival deposit. They have placed the responsibility for retention of these records on the individual agency. That means that any electronic record with an archival requirement in the records retention schedule must be retained in the electronic system indefinitely.

<table>
<thead>
<tr>
<th>Record Series (Records and documentation related to....)</th>
<th>Arch. Code</th>
<th>Agency RRS Item #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transportation studies/proposed project feasibility studies.</td>
<td>R*</td>
<td>TPD05 50TSP06 86PLD02</td>
</tr>
<tr>
<td>Vessel (ferry boats) blueprints, electrical diagrams, revisions</td>
<td>R</td>
<td>MOP03</td>
</tr>
</tbody>
</table>
The records administrator should advise records custodians to change the document status to "Archival Review" for any subject documents during the review and reporting of records eligible for destruction. It may be useful to create and designate a special folder for retaining these documents.

An alternative is to print the records on acid-free paper and forward them to records management for submission to the State Archives. For this alternative, follow the procedures in Chapter 8 to prepare and box records for storage, complete Form 1419, and to ship the records.