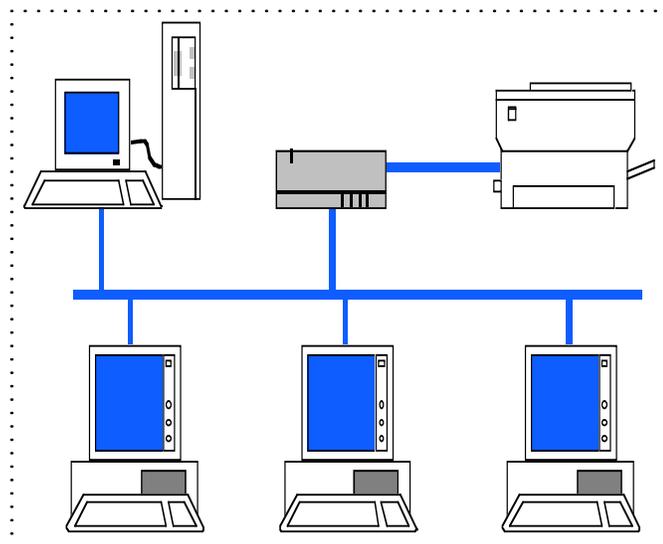


Electronic Records

Introduction

Electronic technology has greatly expanded the methods of creating, editing, maintaining, transmitting, and retrieving state records. Records in electronic recordkeeping systems may now utilize a variety of media from creation to disposition.

One example of an electronic recordkeeping system is one in which the original records are generated on a personal computer and stored on a magnetic disk. While paper copies of the electronic record may be printed out for distribution, the original records are transferred to a minicomputer and stored on magnetic tape. After a specified period of time, the inactive records are transferred to computer-output



Everyday, electronic records become more commonplace in state agencies. The management of electronic records is challenging, but essential to the conduct of state government.



microfilm for long-term storage, and the previous media upon which the records were stored may be erased and reused.

Definitions

Electronic recordkeeping is the operation of a records system in which a computer is required for the user to create, manipulate, or delete records.

Electronic records are stored in a format that only a computer can process and are also called machine-readable or machine-sensitive records.

NOTE: Throughout this chapter the term "record" is used generically, unlike the specific computer science usage referring to a group of related data fields.

Statutory Requirements

The statutory responsibilities of the State and Local Records Management Division and of state agencies to establish efficient, economical management of Texas state government records are set forth in Subchapter L, Chapter 441, Texas Government Code.

Electronic records are clearly included in the statutory definition of a state record. Section 441.180(11) defines a state record as "any written, photographic, machine-readable, or other recorded information created or received by or on behalf of a state agency or an elected state official that documents activities in the conduct of state business or use of public resources."

The agency head is ultimately responsible for an agency's records management program and has the following duties:

§441.183(1) Establish and maintain a records management program on a continuing and active basis.

§441.183(2) Create and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency designed to furnish information to protect the financial and legal rights of the state and any person affected by the activities of the agency.

§441.183(3) Make certain that all records of the agency are passed to the agency head's successor in the position of agency head.

§441.183(4) Identify and take adequate steps to protect confidential and vital state records.

§441.183(5) Cooperate with the Texas State Library in the conduct of state agency records management surveys.

§441.183(6) Cooperate with the Texas State Library and any other authorized designee of the Library in fulfilling their duties under this chapter.



Administrative Rules

The Texas State Library and Archives Commission has adopted administrative rules (13 TAC §§6.91-6.99) establishing standards and procedures for state records in electronic format that have an approved retention period of 10 years or longer (on an agency records retention schedule or in the *Texas State Records Retention Schedule*).

The rules also apply to electronic records identified as having archival value, regardless of how long they are retained in the agency. Compliance with the standards and procedures for electronic records is not required for records with retention periods of less than 10 years but is recommended as a prudent records management practice.



The administrative rules apply to all electronic storage systems, whether on microcomputers, minicomputers, or mainframe computers, regardless of electronic storage media. If an electronic recordkeeping system used for electronic records with retention periods of 10 years or more does not meet the provisions of these rules then the source documents must be retained on paper or microfilmed in accordance with the state *Microfilming Standards and Procedures* (13 TAC §§6.91-6.99).

Program Elements

If a records management program is to be viable and effective, it must be properly placed within the organization hierarchy; management and staff must be aware of their recordkeeping responsibilities and the program's operating systems (electronic and managerial) must be reviewed frequently for efficiency and suitability.

The head of each state agency must ensure that a program for the management of electronic records is established that incorporates the program elements required by the standards and procedures for electronic records.

The program elements required for managing electronic records are the responsibility of the agency head or designated records management officer and include:

- Administering an agency-wide program for the management of records created, received, maintained, used or stored on electronic media.
- Integrating the management of electronic records with other records and information resources management programs of the agency.
- Incorporating electronic records management objectives, responsibilities, and authorities in agency directives.

- Establishing procedures for addressing electronic records management requirements, including recordkeeping requirements and disposition.
- Ensuring that training is provided for users of electronic records systems in the operation, care, and handling of the equipment, software, and media used in the system.
- Ensuring the development and maintenance of up-to-date documentation about all electronic records systems that is adequate to specify all technical characteristics necessary for reading or processing the records and the timely, authorized disposition of records.
- Specifying the location and media on which electronic records are maintained to meet retention requirements and maintaining inventories of electronic records systems to facilitate disposition.
- Appraising the agency's electronic records to develop the agency records retention schedule.
- Securing approval of the records retention schedule and ensuring its implementation for use in the management and disposition of all agency records in all media.



Management Responsibility

Each agency head must either act as or appoint a records management officer to administer the agency's records management program. The records management officer acts as a liaison between the State and Local Records Management Division and the agency.

The role of the records management officer is to coordinate and control the records activity of the agency. The main responsibilities involved in this function are listed here and are discussed in detail in "Records Management Officer" (Part I, *Texas State Records Management Manual*).



The agency records management officer:

- Administers the agency's records management program.
- Assists the agency head in fulfilling all of the agency head's records management responsibilities.
- Surveys or inventories all records of the agency.
- Prepares, submits, and maintains the agency's records retention schedule.
- Disseminates to employees of the agency information concerning state laws, administrative rules, and agency policies and procedures relating to the management of state records.
- Approves all documentation for transfer of records to the State Records Center.
- Originates and approves all requests to dispose of the agency's records.
- Attends training and information classes offered by the State and Local Records Management Division.

Information Resources Management

To the fullest extent practicable, the management of the records, including electronic records, of an agency should be integrated with the agency's management of its information resources. Texas Government Code, §2054.003(6) defines information resources as the "procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors."

The Texas Department of Information Resources (DIR) oversees the activities of state agencies in their management of information resources. DIR has issued adminis-

trative rules and other guidelines to assist agencies in complying with statutory requirements. Copies of these documents are available on request from DIR or at <http://www.dir.state.tx.us> from DIR's web site.

Just as with records management, the head of each state agency is ultimately responsible for the management of state information resources. Similarly, the agency head serves as the agency's information resources manager or may designate another senior agency official to serve in that capacity. The information resources manager serves as the liaison between the agency and DIR and administers the information resources management program within the agency.

The guiding principle in information resources management is that information should be managed as an important asset. The State and Local Records Management Division also recognizes the importance of the records of Texas state government as a resource for citizens as well as public officials. State records may provide proof of a particular action, contain evidence to protect the rights of individuals or the government, and provide decision support which is valuable to the progress of state business. Whatever their content, records created and received in the course of government business are significant to Texans.

The Paperwork Reduction Act of 1980 requires federal agencies to consolidate the responsibility for all records management functions, including electronic recordkeeping, with other information resources management functions in a single agency official. With this decision-making authority, the official can delegate responsibility for an electronic recordkeeping program to a specific group of individuals if the size of the organization warrants it. This group might have the authority to review, analyze, and decide any number of electronic recordkeeping issues. The important factor is to ensure that responsibility and decision-making authority are not fragmented throughout a federal agency.

Texas has no comparable requirement that the records management officer, who is responsible for records management, have decision-making authority for





information resources management. But the need for coordination of these functions within the agency is absolutely essential. If the person designated as the records management officer is not the same person named as information resources manager, it is imperative that these individuals work together to coordinate records management and electronic recordkeeping activities.

Agency Directives

It is extremely important that electronic records management objectives, responsibilities, and authorities be incorporated in appropriate agency directives. Managers and staff must be aware of their recordkeeping responsibilities. Managers of state programs utilizing electronic records have the responsibility of instructing employees in the creation, use, and disposition of electronic records and of ensuring that such procedures are followed.

Some organizations permit each user of electronic equipment to operate independently with no established policies or standardized procedures. This tendency may not have serious consequences in small organizations, but if the practice is allowed to flourish in larger operations, the situation may become chaotic. Valuable records can be lost, altered, or destroyed; and the electronic recording medium can be inadvertently obliterated or overwritten. Along with these hazards, there is the distinct possibility of unauthorized access to sensitive or confidential information in electronic files.

All persons who use electronic recordkeeping equipment to create, retrieve, edit, store, transmit, and dispose of electronic records are responsible for correctly using the equipment, managing the records according to prescribed procedures, and seeking assistance whenever they have questions concerning the system and its operation.

Records Management Review

The records management officer should establish procedures for the periodic review of electronic records management requirements and issues.

The information resources manager and other agency managers for electronic recordkeeping, in cooperation with the records management officer, should regularly evaluate how efficiently information is stored and retrieved using present equipment, networks, and software. They should study future requirements and recommend new systems as appropriate.

Certain factors should be considered before a new or upgraded electronic recordkeeping system is purchased and put into use. These factors affect the practicality, the cost, and the effectiveness of new configurations.

The Department of Information Resources (DIR) should be consulted for specific requirements affecting the process for acquiring information resources technologies. DIR can assist agencies in evaluating proposed technology and planning acquisitions. If significant changes are being considered in electronic recordkeeping, it is recommended that an agency contact both a DIR systems analyst and a government records consultant from the State and Local Records Management Division.

Training

In cooperation with the agency's information resources manager, the records management officer should ensure that appropriate training is made available for users of electronic records systems in the operation, care, and handling of the equipment, software, and media used in the system.

Training for individuals who create, edit, store, retrieve, or dispose of records is an important aspect of electronic records management. Training should enable agency





personnel to identify state records, understand how records are filed in an electronic recordkeeping system, how records are safeguarded, what procedures are used to edit records, and how records should be disposed of according to legal requirements.

Methods of providing training for the use and management of electronic records could include one or more of the following:

- Classroom training, offered several times a year on a recurring basis or as needed for special situations. This is the type of training available to the largest number of state agencies because the State and Local Records Management Division has a regular schedule of classes on a variety of records management topics.
- A self-learning center within the agency, where operators can teach themselves at their own rates of learning through interactive programs. The commercial tutorial programs do not usually include records management information, but tutorials teaching records management concepts for electronic records could be developed by the agency.
- Telephone “hotlines” or “help desks” staffed by knowledgeable computer support professionals within the agency who can answer technical questions and provide “quick fix” solutions. This process may not be an adequate learning tool for good records management unless the computer support professionals have received specialized records management training.
- Training offered by the manufacturer or vendor— This usually covers the operation of computer hardware and software but does not include records management concepts. The Department of Information Resources manages the state contract which offers vendor training at discount rates.

NOTE: The training schedule for State and Local Records Management Division classes is distributed to all agency records management officers. A copy of the schedule may be requested from the division or downloaded at <http://www.tsl.state.tx.us/SLRM/SLRMhome.html> from the agency's web site.



Documentation

Working with the agency's information resources manager, the records management officer should ensure the development of up-to-date documentation about all agency electronic records systems that is adequate to specify all technical characteristics necessary for reading or processing the records and the timely, authorized disposition of records. Documentation includes written descriptions and procedures that provide information about a computer program or a computer system so that it can be properly used and maintained. The documentation should also:

- Identify all defined inputs and outputs of the system.
- Define the contents of the files and records.
- Determine restrictions on access and use.
- Provide an understanding of the purpose(s) and function(s) of the system.
- Describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information.

Records Inventory

The records management officer must determine the location and media on which the electronic records of the agency are maintained in order to ensure that records retention requirements are met.



Each agency must complete a records inventory and keep it updated. The records inventory is a complete listing of the records holdings in an agency including convenience copies. It identifies all records, including where they are located and on what medium (i.e., paper, microfilm, electronic).

“Records Scheduling” (Part II, *Texas State Records Management Manual*) describes the records inventory process, which is applicable to electronic records as well as records in other formats. Electronic records may be maintained on magnetic storage media (magnetic tapes, cartridges, floppy disks, and diskettes), on-line, or on optical media. The record copy of information processed on the computer may also be in the form of data processing printouts or computer output microfilm.

With a mainframe or minicomputer operation, there may be databases that have multiple outputs. The outputs may create several records series because they are produced for separate divisions, the data is summarized differently, and the retention periods vary because of specialized use. For example, an agency may have an automated database for client information. One division uses it to do research and prepare administrative reports which are maintained for three years, then reviewed for archival value. Another division uses the same database for case management computer printouts which are maintained for five years to meet federal reporting regulations. As records are inventoried in each division, each of these records series would be documented on an inventory worksheet.

There could also be a situation in which a database is created for one function. For example, a database of fiscal information may generate several reports, but if they all have the same use and the same retention period, they can be grouped as one records series.

Appraising Records

Once electronic records have been inventoried, they must be appraised. Appraisal is the process of using the information gathered during the inventory to analyze each records series and develop a retention schedule.

The first step in determining recordkeeping requirements for electronic records is to identify the creators and users of the records. In doing so, it is important to remember that records may be used by different individuals and offices within an organization for different purposes. Some records may exist in several formats within one office. If such records are needed for separate program purposes, recordkeeping requirements may differ for each purpose. Such requirements, determined during the records inventory, will be significant factors in deciding where, in what format, and for how long the records are maintained.



In addition to the information gathered during the records inventory, the *Texas State Records Retention Schedule* (RRS) is a resource that will be of primary assistance to an agency during records appraisal. The RRS includes electronic data processing records with required minimum retention periods for records series that are often maintained by state agencies and are related to electronic recordkeeping.

The function of a records series is the primary consideration when determining classification or retention periods. For example, records series item number 5.1.004 (Category 5: Support Services Records) is the appropriate classification for mailing lists; the retention period for mailing lists is “until superseded.” This classification and retention period are applicable to all mailing lists, whether the record copy is maintained electronically or on paper.

Appraising electronic records for records management purposes includes identifying the record copy vs. drafts and convenience copies. Drafts or working documents are normally kept only until the final draft is approved. Previous revisions are then erased and only the final text is kept. However, a draft version containing information not included in the final version, but useful for preparing similar documents in the future, could be retained as a convenience copy.

A document maintained in electronic format may be only a convenience copy as the record copy is in the form of paper or microform. For example, correspon-



ence may be kept on personal computers for the convenience of creating another letter, or information in an automated database may be maintained as the record copy in computer printout. If the only copy of the information is in electronic format, then it is the record copy. If the record copy was in another format that has been destroyed and the electronic information has not been destroyed, then the electronic file becomes the record copy by default.

NOTE: Convenience copies of documents should be kept only as long as needed to meet the purpose for which they were created, and no longer than the record copy. This requires a knowledge of where the record copy is being maintained in the agency and procedures to inform staff on the proper disposition of records.

Appraisal decisions on the retention of the record copy include:

- Total retention period each records series will be maintained based on administrative, fiscal, legal, and historical values.
- Length of time a records series will have current, active use in the agency.
- Length of time a records series should be stored if there is a period of inactive use prior to final disposition.
- Appropriate format for a records series while it has current use and during any inactive storage.
- Potential archival value of a records series.
- Security classification of a records series (open or confidential based on the Texas Public Information Act).
- Identification of vital records.

During the appraisal process, any special concerns for electronic records should be addressed. For example, plans for records in electronic format that have potential archival value should be discussed with the staff of the

Archives and Information Services Division, Texas State Library. See “Final Disposition” (Part IX, *Texas State Records Management Manual*) for guidelines on identifying historical records.

The State Archives does not accept records that are stored on magnetic or optical media because of the potential for problems with the hardware and software dependence of these media, and questions about their playback stability for the permanent preservation of records. When records having historical value are no longer needed for the current business of the agency, they must be transferred to the Archives and Information Services Division on paper or microforms.



Records Retention Schedule

Part II of the *Texas State Records Management Manual*, “Records Scheduling,” explains the statutory requirements and procedures for developing, submitting, approving, and updating the records retention schedule. Use of the “Records Retention Schedule” (SLR 105) form is required for all state agencies.

The “Certification and Approval” (SLR 105C) form must be submitted with the agency’s records retention schedule. After the schedule is reviewed and approved by the State Auditor and the Director and Librarian of the Texas State Library, it is returned to the agency and used as a basis for management and final disposition of the records series listed.

NOTE: Convenience copies of records series do not have to be listed on the retention schedule since it is not necessary for them to be maintained the full length of the retention period. For example, if the record copy of “administrative correspondence” is listed on the records retention schedule as paper and there is also a convenience copy on the computer, the electronic copy does not have to be listed. However, agency staff should know that convenience copies should be destroyed as soon as they are no longer needed, and that they cannot be kept longer than the record copy.



Special Concerns

The remainder of this part of the *Texas State Records Management Manual* provides further information on the management of electronic records from creation of the records, throughout their use, to their final disposition. In addition to the basic records management program requirements that apply to electronic records, there are other special concerns for managing electronic records throughout their life cycle.

Creating Text Documents

Electronic records systems that maintain the record copy of text documents or data used to generate the record copy of text documents on electronic media must meet the following minimum requirements in accordance with the state *Electronic Records Standards and Procedures* (13 TAC §§6.91-6.99):

- 1) Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system.
- 2) Provide security to ensure integrity of the documents.
- 3) Provide a standard interchange format when determined to be necessary by the agency to permit the exchange of documents on electronic media among the components of the agency using different software/operating systems.
- 4) Provide for the disposition of the documents including, when necessary, the requirements for transferring archival records to the State Archives.

The standards and procedures for electronic records also require that a document created on an electronic records system must be identified sufficiently to enable authorized personnel to retrieve, protect, and carry out

the disposition of documents in the system. Agencies must ensure that records maintained in such systems can be correlated with related records on paper, microform, or other media.

Organizing Computer Files

When electronic records are created as documents on personal computers, records management principles should be applied to ensure appropriate recordkeeping practices. The personal computer is a storehouse of information, but the usefulness of electronic records is directly impacted by how they are organized. The accessibility of electronic document files and the efficient management of records in electronic format will be enhanced by:

- Grouping files functionally into records series.
- Arranging files in a logical order.
- Standardizing file names.

Grouping by Records Series

Electronic files are created and stored on a personal computer hard disk which holds large numbers of computer files just as a file cabinet holds large numbers of paper files. Paper files are organized into records series. A records series is a group of identical or related records that are normally used and/or filed as a unit, and are evaluated as a group for retention scheduling purposes.

This functional records series concept also applies to electronic records on the personal computer. Paper files are arranged by records series in file cabinets which have drawers and file folders. Similarly, electronic files should be arranged into records series on the personal computer, based on program and activity functions.





For Disk Operating Systems (DOS), files are organized by using tree-structured directories in which major groupings of files are given a directory name and subgroupings of files in directories are given subdirectory names. The result is a hierarchical classification of information from general to specific that allows files to be grouped according to function. Those files with similar uses can be organized together, while files with entirely different uses can be placed in different directory structures or paths.

The primary advantage of a system using a tree-structured directory is that searches and retrievals can be made from a specific directory or subdirectory rather than having to access all of the files for every operation.

Personal computers with other operating systems use comparable means for organizing a hierarchical grouping of electronic records by providing for the creation and naming of documents which are filed into folders, and then by organizing folders within folders.

Careful consideration is needed in the grouping of records and in the selection of a title which appropriately describes the function of the records series. If the electronic files are convenience copies, the records series titles should be the same as those used on the retention schedule for the record copy in order to facilitate appropriate disposition.

Arranging in a Logical Order

On the personal computer, electronic files can be logically ordered within records series by any of the arrangements commonly found in filing systems:

- Alphabetically (name of person, place, subject).
- Numerically (social security number, project number, date).
- Alpha-numerically (a combination of letters and numbers, such as an abbreviation of a name and a date).

Part IV of the *Texas State Records Management Manual*, "Filing Systems," describes each of the three basic filing arrangements. Because each filing system has certain advantages and limitations, guidelines are provided for selecting an appropriate system based on characteristics of the agency's records practices and needs.

NOTE: To make the best use of a computer's capabilities, the filing of electronic records in an agency should be coordinated and made compatible with the filing system for paper and/or microfilm records. In any organizational unit there must be cooperation in the use of common assets, and electronic information is a critical asset.



Standardizing File Names

All computer operating systems require that new files be given file names in order to be saved on the storage media of the computer. The most common personal computer operating systems have an eight-character file name followed by a decimal and then a three-character extension that normally identifies the type of file. For example, a word processing file might have the file name and extension "EXAMPLEA.DOC." The electronic backup copy of this file would have the same file name but a different extension "EXAMPLEA.BAK."

Some software automatically creates file name extensions based on the software used to create the document. Others allow users to create, add, or leave out extensions. Since file names must be unique, whereas file name extensions are common to the file types, sorting files by file name extension is a useful feature in electronic records management. This is used as a means of locating and arranging general types of files.

Computers use file names for operations that list files, delete files, copy files, compare files, and look at the contents of files. For these operations, most computer operating systems allow the use of global file name characters to search for groups of computer files. For example, with almost all Disk Operating Systems (DOS), the character "?" in a file name search means that any valid character can occupy that position.



The file name EXAM?88 would refer to any file that starts with EXAM and ends with 88, such as EXAM88 or EXAM388. More generally, the "*" wildcard character indicates that any character can occupy that position and all the remaining positions in the name. In an eight-character node system, the search term EXAM* would refer to all files which begin with "EXAM" such as EXAMS88, EXAMS89, or EXAMPLEB.

The use of global file name characters to search for groups of files can be exceedingly productive if a naming convention has been developed to take advantage of group processing. This means that the position of the characters in the naming convention must be standardized, each group of characters must be completely defined, and the names must conform by position to the convention specifications.

For example, an agency with a Construction Engineering Division might have a file-naming convention that designates the first two characters as the division code (CE), the next four characters as the last four digits of the project number, then a two character abbreviation to identify the type of file; e.g., CP for construction plan. Thus "CE5829CP" could be the file name for the construction plan file, project #45829. Groups of construction plan files would then be easily identified using global file name characters. It is important to remember to use all four digits for the designation of a year to avoid problems as we move into a new century.

There are many benefits to standardizing the terminology used in naming electronic files.

- Accessing files easily and rapidly.
- Training new employees in less time.
- Avoiding the loss of information.
- Naming files quickly and easily.
- Sharing files more easily.
- Identifying groups of files eligible for disposition at the same time.

Electronic Records Integrity

Various functions of the operating system may affect the status and integrity of records created on a personal computer. Saving the file being created is one of these functions. A new file must be saved properly, or it will be lost when the computer is turned off or the application is quit.

Saving the previous version of a file is another specified function because the previous version is often replaced with the new one. This is an example of the importance of file names as previously discussed. If the operating system automatically makes a backup copy of the previous version, it will be differentiated by a distinct extension, such as BAK and DOC. But if two records have exactly the same name, one would be replaced by the other.

Copying and erasing files on the personal computer can have a direct impact on electronic records integrity. Users must know how the operating system works to save files, and they should think about how the computer's file-save feature will affect the work being created. For example, when a file already exists on a specific medium, such as the hard disk, under a specific file name/extension, e.g., "SAMPFILE.DBM," a revision of that file may replace the old file. If the user does not want to change the previous version, the file can be copied to a diskette so that two versions of the file are then available, the current one and its predecessor.

A problem in file management can arise when the copy procedure accidentally occurs in the wrong direction. If a user makes a backup copy onto a removable medium (such as a diskette) and then loads the backup copy from the diskette onto the hard disk, the preceding version of the file may replace the current file.

When files have been erased individually, by file name, there is normally no problem with records integrity. The user clearly intended to erase that individual file. However, users should be aware that the record is still on the hard drive, for example, even though it is not shown on





the file directory. This can create a potential security problem for confidential or sensitive records if users do not follow appropriate procedures for disposing of electronic records.

It is important for personal computer users to keep in mind that they may be creating, manipulating, and deleting official state records. (The authorized process for final disposition of records, including recommendations for disposing of electronic records on magnetic media, is discussed later.)

Database Management

Creating electronic records as text documents on a personal computer is one way of electronic filing. Another type is database management. A database is a collection of data that forms the basis of an activity. The two elements essential to a database are coherence and organization. Coherence means the data are related to a specific activity or purpose. Organization means the data are related in such a way that users can meaningfully access parts of the database.

Some limitations of database management are:

- Cost of developing databases.
- Cost of the necessary equipment and software.
- Need for additional expertise to administer and operate the electronic system.
- Cost of maintaining duplicate systems (in many situations) when paper or microform documents cannot be replaced by electronic files because of legal or historical requirements.

Database Applications

Automated recordkeeping systems have been developed which use database management applications for specialized records management functions. Those being used or considered for use in state government include:

- Computer Output Microfilming (COM).
- Computer Output to Laser Disk (COLD).
- Computer-Assisted Retrieval (CAR).
- Electronic-Based Records Management Systems (EBRMS).
- Optical Disk Systems (ODS).



Computer Output Microfilming

Computer output microfilming is an automated recordkeeping process which converts machine-readable, computer-processible database information to a human-readable textual or graphic record on microfilm without first creating paper documents.

A computer output microfilmer, or COM recorder, is a computer peripheral device and is capable of either on-line or off-line operation. In an on-line system, the data is transmitted from the computer directly to microfilm in the same way that it would be transmitted to a display screen or a printer. In an off-line system the data is transmitted to another device, such as a computer tape or a disk. With an off-line system, the data can be retrieved and converted to an image for editing before converting the image to film.

Most COM recorders output records to 4" x 6" sheets of microfilm. At a 48X reduction ratio, one sheet of COM film contains 269 images and one index frame. For computer applications requiring the timely production



of voluminous printed reports from machine-readable data, COM recorders are used as high-speed, paperless replacements for line printers. The obvious advantages of computer output microfilming are speed of creation and reduced costs for storage and distribution of information, especially if paper copies are eliminated. It is also an archival media and its legal acceptability is well established.

Computer Output to Laser Disk

COLD is the process of transferring computer output directly to a laser disk storage device. COLD systems are software and hardware solutions that use optical disks to store, index and retrieve formatted computer output, and are alternatives to COM as a storage and retrieval mechanism.

Indexing and retrieval software is an important consideration in COLD applications. Boolean and keyword searching allow retrieval of desired information in a fraction of a second. COLD systems can be PC/LAN based, client server based, and host (mainframe) based. One advantage to COLD technology is that optical disks have high storage capacity combined with low media cost. Each page can be accessed in sub-seconds. Data can be manipulated through "cut and paste" processes. COLD also allows concurrent access and advanced sorting capabilities. The need to exchange platters in jukeboxes is the biggest obstacle to retrieval performance. COLD technology is still evolving and the need for upgrades may be fairly continual. The write speeds of optical disks are far slower than magnetic disk.

Computer Assisted Retrieval

Broadly defined, computer-assisted retrieval (CAR) denotes an automated document storage and retrieval technology that uses computer hardware and software to index and locate documents or document images

recorded on any media. CAR systems use database management software to create, maintain, retrieve, and manipulate index information accompanied by pointers to document locations or by unique document identifiers. At retrieval time, the index is searched to determine the existence and storage locations of documents pertinent to specific information needs.

While computer-assisted retrieval concepts can be applied to paper documents and to document images recorded on magnetic or optical media, the most common use of CAR in state government is with systems that utilize microforms for document storage. This use of computer-assisted retrieval combines the space savings and other advantages of microform storage with the ability of computers to rapidly retrieve index information. From the computer standpoint, the CAR approach simplifies data entry and on-line storage by limiting those activities to index data rather than entire documents.

A computer-assisted retrieval system that is microform-based includes computer and micrographic subsystems. A CAR system's computer components support the entry, maintenance, and processing of index records that are linked to document images stored by the micrographic subsystem. The computer subsystem includes a central processor, a display unit with keyboard, and sufficient magnetic disk capacity for on-line storage of database records, supporting files, and CAR software. Optional hardware components include a printer and telecommunication links to other computer systems.

Electronic-Based Records Management

In an electronic-based records management system, the computer is used to manage records without altering the format or storage of the records. The EBRMS tracks records in multiple media throughout their life cycles, provides appropriate reports, and allows queries of records.

An efficient electronic-based records management system should be able to accurately describe the status





of records in terms of their location and characteristics. The system also contains action prompts that tell when to purge, transfer, and alter the status of records. To fulfill these requirements, a EBRMS produces routine system reports, such as:

- Records by retention status.
- Records by type (vital, active, inactive, archival).
- Records by location.
- Records by security classification (open or confidential).
- Records to be placed in inactive records storage.
- Equipment location.

The development of an electronic-based records management system to index files and records in all media formats (e.g., electronic, paper, microfiche, microfilm, tapes) can help an agency to locate, retrieve, and share files in central and decentralized locations. The computerized master index for records brings together information on each file as well as on files in every location, provides faster retrieval time, facilitates accurate maintenance of statistics on activity rates, and enables better records management planning.

Some of the functions that electronic-based records management systems perform are keyword indexing/searches, records location management, records retrieval assistance, automated file label creation, retention schedule maintenance, records inventory, box/file/record tracking, and destruction notifications.

Optical Disk Systems

Optical disk systems (ODS) are automated systems that utilize optical media for electronic storage. ODS applica-

tions include the storage of computer-processible data, and electronic imaging systems that store digitized document images.

The state *Electronic Records Standards and Procedures* (13 TAC, §§6.91-6.99) permits state records with an approved retention period of 10 years or more to be maintained in electronic format only, including storage on optical disks, provided that the agency is in compliance with the administrative rules. Agencies currently using or considering the use of optical technology should pay particular attention to the following sections of the standards and procedures for electronic records that have requirements for optical media:

§6.96(b)—Storage areas for backup optical media must be maintained within the temperature and humidity requirements, specified in the international standard referenced by this section (14°F to 122°F temperature and 10% to 90% relative humidity).

§6.96(c)—Data maintained on optical disks must be recopied a minimum of once every 10 years.

§6.96(g)(1) through (11)—Electronic records stored as digital images on optical media must meet the requirements under “Maintenance of Electronic Records Storage Media” in this section.

§6.98(c)—The court ordered expungement of information recorded on an optical Write-Once-Read-Many (WORM) system must be implemented according to the specifications listed in the standards and procedures for electronic records.

Records series to be stored on optical disk must be listed on the agency records retention schedule; the schedule must be approved by the State Auditor’s Office and the Director and Librarian of the Texas State Library and Archives Commission. The records series medium on the records retention schedule must be coded with an “E” (for electronic) in Field 10 of the “Records Retention Schedule” (SLR 105) form.





Optical disks containing state records, whether original or preservation duplicates, and other original record media that have been converted to optical disk will be accepted into the State Records Center based on existing storage eligibility criteria. See "Records Center Services" (Part VIII, *Texas State Records Management Manual*) for additional information.

Maintaining Electronic Records

Electronic recordkeeping has a very useful operational value for agencies. Computers are excellent for manipulating data and creating documents, especially the easy revision of text. Electronic recordkeeping also has its potential hazards and limitations. The following important aspects of using electronic records should be given special consideration:

- Security requirements for electronic recordkeeping systems.
- Care of storage media.
- Legal issues related to using electronic records as evidence.

Security of Electronic Records

Texas Government Code §441.184 requires the agency head to identify and take adequate steps to protect confidential and vital state records, regardless of medium. The state *Electronic Records Standards and Procedures* (13 TAC, §6.95) specifies the following requirements for the security of those electronic records subject to the rules. State agencies must implement and maintain an electronic records security program for office and storage areas that:

- 1) Ensures that only authorized personnel have access to electronic records.
- 2) Provides for backup and recovery of records to protect against information loss.

- 3) Ensures that personnel are trained to safeguard confidential electronic records.
- 4) Minimizes the risk of unauthorized alteration or erasure of electronic records.
- 5) Documents that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.



A duplicate copy of vital records and any software or documentation required to retrieve and read the records must be maintained in a storage area located in a separate building from the building where the records that have been copied are maintained.

For all permanent records stored on rewritable electronic media, the system must ensure that read/write privileges are controlled and that an audit trail of rewrites is maintained. Other considerations include backward compatibility and life expectancy of the media.

Hardware and Data Security

Security for the electronic records created, used, and stored on computer systems is an important issue that needs to be thoroughly considered by agencies, in addition to the specific standards and procedures required by the administrative rules of the Texas State Library and Archives Commission. Mainframe computer systems have traditionally had considerable protection, but personal computers have not because they have been treated as single-user devices. As a result, security weaknesses may threaten the confidentiality, integrity, or availability of electronic information.

There are two major means of protecting electronic records:

- 1) Physical security of the computer hardware.
- 2) Securing data by controlling access.



Hardware concerns—Computers and their component parts are high-value items. A security policy should be established that will protect computer installations. Mainframe computer operations should be in an area which is locked, has constant attendance and supervision, and is restricted to authorized personnel.

For personal computers, possible solutions to protecting the hardware are central processing unit cabinet locks, cables to lock equipment to stable fixtures, bolt-down devices to permanently attach personal computers to desks, keyboard locks, workstation enclosures, and alarms to signal motion. Rooms in which the hardware is located should be locked when they are not occupied.

Data concerns—A good security system for protecting electronic data will employ a number of different products, services, and resources which should be customized to an agency's particular needs. Not every system or device is appropriate for all agencies. Those responsible for implementing security systems must weigh the potential costs of suffering a data loss. Then you can consider the value of each method and develop a complete security system that is tailored for your situation. In order to be successful, computer security has to be an on-going management concern.

The following are some of the common methods of data security that can be employed to customize a security system.

Risk analysis—Software packages are available to help quantify potential exposure to security breaches. This is a good starting point in assessing your need for security and developing a plan of action.

Access levels—Users can be assigned a variety of access privileges, such as read only, remote access, specific file or directory access, and ability to upload or download data from a mainframe or network database.

Passwords—Passwords can be used to control access to terminals, files, records, or even fields within a record. In a password system, users must enter the appropriate password to gain access to the data for which they have

been cleared. Multiple levels of passwords can provide entry to different layers of information in an agency database. The best approach is to use passwords to create a hierarchy of entry and progressively more complex entry codes as the information becomes more sensitive. Passwords should be changed every one to two months for adequate security to be maintained.

Callbacks—Callback devices prevent unauthorized access to the communications channels of a computer. Some devices require a caller to provide an identification number and hang up. After verifying the user's access rights, the device calls the user back. When combined with a password, the system requires that the correct user identification also be provided from a specific location (modem number).

Audit trails—Security software programs can audit computer use by providing a comprehensive record of all network or system activity, including who is accessing what data, when, and how often.

Encryption—Data encryption is a process that “scrambles” data when they are stored or transmitted. Data so treated become unintelligible without a data “key.” When the encrypted data are sent to another terminal, the required software key on the receiving end decodes the information. The use of encryption can be a complex process and should be used only for data that are highly confidential and require the utmost security.

Data backups—Backing up disks will be discussed as a common-sense measure to safeguard data in the event of loss through disaster. Data backup is also an important safeguard should an unauthorized user access and change an electronic file or document.

Security levels—Distinguishing the levels of security for records (confidential, restricted, or open) is useful for determining each records series' appropriate level of protection. Access by the public to records in the custody of state agencies is covered by the Public Information Act (Texas Government Code, Chapter 552).





NOTE: Electronic records that are confidential because of an exception to the Public Information Act or because of federal regulations or law, such as the Privacy Act of 1974, should not be maintained on computers which can be accessed by unauthorized users.

Environmental Considerations

The effects of environmental conditions—humidity, temperature, and cleanliness—on recordkeeping system components are a security concern because of the potential loss or alteration of records maintained electronically.

A large scale recordkeeping operation maintaining great numbers of sensitive records on a large computer will require extensive environmental controls. A smaller scale, non-critical recordkeeping system operating on a personal computer will probably involve fewer environmental considerations. However, small systems with sensitive electronic equipment require at least a minimum level of environmental control to operate reliably.

The state *Electronic Records Standards and Procedures* (13 TAC, §6.96) requires that the storage areas for electronic media must be maintained within the following temperatures and relative humidities:

- 1) For magnetic media—65°F to 75°F and 30% to 50% relative humidity.
- 2) For optical disks-storage environmental—14°F to 122°F and 10% to 90% relative humidity, as specified in *Information technology—130mm optical disk cartridge, write once, for information interchange* (ISO/IEC 9171-1, 1990 or latest revision).

Disaster Preparedness and Recovery

In addition to the maintenance of electronic records, attention should be given to preparing for disasters. Agencies need to develop plans for coping with emer-

gency situations—from minor disruptions to major disasters—to ensure the continued operation of electronic recordkeeping systems.

The whole idea of disaster recovery planning is to think about and plan for potential misfortunes before they happen. For example:

- How likely are they to happen?
- What can be done if they do happen?
- What can be done to lessen their likelihood?
- What can be done to prepare for these events?

Assessment of emergency situations—Emergencies can range from a temporary disruption of power to complete destruction of an office. Planners must determine which of the types of emergencies are most likely to disrupt their operations and shape emergency response procedures and recovery planning to expected situations. Not every emergency can be classified as disaster, but personnel prepared for a disaster can successfully cope with lesser emergencies.

Commonly, the severity of an emergency is defined by four levels of disruption:

- 1) Limited—A temporary interruption with no damage or data loss can be classified at this level. Examples would be a power failure or fluctuation, a communications failure, evacuation of a site because of a bomb threat, or the unavailability of key personnel.
- 2) Serious—Repairable damage to equipment or the office area or replaceable loss of key people, data, records, or software could be considered a serious disruption. Examples would be an equipment breakdown, a failure of the air-conditioning system, or minor damage because of sabotage, vandalism, theft, or human error.





- 3) Major—Destruction of equipment or office area or of data can be classified as a major disruption. Examples would be a complete loss of equipment because of water damage, explosion, or structural mishap; or an accidental or deliberate loss of data.
- 4) Catastrophic—This category includes the total loss of office area or equipment, data, or people. An example would be the complete destruction of the office and the loss of personnel because of fire or a natural disaster.

Disaster recovery—Contingency plans must be broad enough in scope to cope successfully with the immediate emergency, provide interim service, and bring the electronic recordkeeping function back to normal. Because an organization must respond quickly to a disaster, recovery procedures must be spelled out clearly.

The people most likely to execute an emergency plan are the ones who develop it. However, office workers may be incapacitated and unable to function following a disaster. Therefore, the plan should be written so that others less familiar with the office will have the information they need to continue operations.

A disaster resulting in major damage, so that an office and/or equipment are no longer usable, may require backup operations be conducted at a new location until repairs are completed or services can resume. A state-owned disaster recovery operations center is managed by the Department of Information Resources to support recovery operations in the event of a disaster to a state agency's telecommunications or information systems.

The Texas Department of Information Resources is responsible for statewide disaster recovery planning for information resources and has established minimum security standards for the protection of automated information resources by state agencies, as adopted in 1 TAC 201.13(b). To assist in the interpretation and implementation of these standards, the department has developed the *Information Resources Security and Risk Management Policy, Standards and Guidelines*

manual, which is available on request from the Department of Information Resources or can be downloaded at <http://www.dir.state.tx.us> from their web site.

Planned backup of electronic records—Part of the disaster recovery plan should be the planned backup of agency electronic records. Several methods of performing backups are of use for different levels of data protection. The most important factor in a backup program is to do it regularly.

“How often should I do a backup?” is a common question. The answer is a subjective one, but it can be safely said that the interval between backups is determined by the amount of work you are willing to do over and the potential consequences for the organization if the data is lost. A rule of thumb in general usage is every eight hours. Thus if the computer is used all day long, then backup at least daily. If eight hours of data creation are done in a week, then back up weekly, and so on. When users share a personal computer, they should be encouraged to back up their files more often, preferably after every update.

As important as regular backups is labeling backup media accurately so that the following information is available for system restoration:

- Name of the organizational unit responsible for the records.
- Descriptive title of the contents.
- Dates of creation.
- Security classification.
- Identification of the software and hardware used.
- System title, including the version number of the application.

Additional information that must be maintained for electronic media used to store permanent electronic records is outlined in the state *Electronic Records Standards and Procedures* (13 TAC §6.96).





To be accessible in case of disaster, backup media must be stored in a carefully planned manner. Not only must records be backed up and stored, but agencies must also have copies of current versions of application software for vital systems and up-to-date operations manuals, systems documentation, program documentation, and operating system tapes or disks. The best protection for backup copies of electronic media is off-site storage and this is specifically required for vital records, as stated in 13 TAC §6.95(b) of the state *Electronic Records Standards and Procedures*.

The State Records Center offers disaster recovery storage services on a cost-recovery basis to state agencies in the Austin area. Electronic backups can be picked up at an agency, as often as once a week, and stored at the State Records Center in a vault designed to specifications for magnetic media. Contact the State and Local Records Management Division for additional information.

Care of Storage Media

How electronic records should be stored depends on their use. The maintenance of electronic records is similar to paper records. Current records are actively used in the office for the day-to-day operations of the agency. There may also be a period when active storage is needed. The two primary types of storage media for electronic records are magnetic and optical. Magnetic media, commonly used for storage of state records, include hard disks, diskettes (floppy disks), and magnetic tapes (cartridges).

Hard Disk Maintenance

Hard disks offer on-line, immediate access to electronic records. A hard disk's advantages over a diskette are its speed, storage capacity, and durability. While similar to a floppy disk in magnetic surface, hard disks are solid and can spin much faster than diskettes. However, because of the extremely close tolerances used in hard drives, the smallest pieces of dust or smoke can damage the disk and cause data loss. This can also occur if a com-

puter is subjected to rough handling. If the read/write head makes contact with the disk, the recording surface of the disk can be scratched resulting in a loss of data (sometimes called a head crash).

Always move the computer with care. Most hard disks provide a designated landing zone on which the disk head can be parked when moving the system to reduce the risk of a head crash. Some systems automatically park the head each time the system is turned off. The documentation for the computer should include specific instructions for protecting the hard disk during a move.

Another potential problem for hard disk usage is fragmentation. Through the daily creation and deletion of files, the data on hard disks becomes fragmented, which decreases disk performance (speed) and could eventually result in a head crash. Operating system instructions should include procedures for reducing fragmentation. There are commercial utilities which are simple and easy to use to “tune up” the hard disk.

NOTE: The information recorded on a hard disk is subject to error, or even total loss, if a device that emits a magnetic force is placed near the computer’s hard disk. This also applies to electronic records stored on all types of magnetic media.

Diskettes (Floppy Disks)

The disaster recovery team should be contacted and assembled prior to the start of work to salvage records after a disaster. The team members must be briefed on the procedures to be followed and the priorities to be met. Each person should be given a specific area of responsibility. No salvage activity should begin until a plan of action has been determined by the team leader.

One of the immediate priorities for the action plan must be to obtain the various services, equipment, and supplies needed during the salvage operation. The disaster plan should provide most of the basic information; however, it may be necessary to spend





considerable time on the telephone. A communications center should be established immediately, which can function as a centralized point for the organization of the recovery effort and to help avoid confusion and delays whenever possible.

Arrangements must also be made to take care of the needs of all personnel involved in the recovery effort. Hot coffee/tea and food should be available in an area where people can rest and relax, separate from the disaster area.

Magnetic Tape and Cartridges

Magnetic tape and tape cartridges are generally associated with mainframe or minicomputer operations rather than personal computers. But the records residing in personal computers are increasingly being transferred to tape cartridges, or "streaming tape," for a backup copy instead of diskettes being used for this purpose.

Like the surface of diskettes and hard disks, magnetic tape is coated with an emulsion of magnetic oxide particles. Other chemicals are also used in the manufacturing process to give the tape good operation characteristics, such as flexibility, conductivity, and softness.

Computer magnetic tape is a fragile medium, highly susceptible to the generation of error by improper care and handling. The complete care and maintenance of magnetic tape can be a complicated and involved process. Even under ideal conditions of controlled storage, magnetic tape is not expected to retain data in a readable state any longer than 10 years.

- NOTE: The maintenance requirements for electronic
- media are listed in 13 TAC §6.96 of the state *Electronic*
- *Records Standards and Procedures*. These specify the
- environmental conditions that must be provided and
- outline mandatory provisions for pre-testing, recopying,
- sampling, and labeling electronic media.

Optical Media

A new technology, which offers the advantage of on-line access to electronic records, is the use of lasers to record and read data on optical media. Optical storage systems provide a supplement, complement, or alternative to magnetic storage media in a broad spectrum of data and document image storage applications.

These systems permit the direct recording of information generated by keyboards, document scanners, and other input devices. They can also record information transferred from magnetic media and other optical media, or downloaded from a mainframe. Optical media offer much higher storage capacities than magnetic media of comparable size and are well suited to electronic imaging systems, video storage, and other image-oriented applications that require storage space for huge quantities of data.

Optical storage systems include both equipment and media. Optical recording and playback equipment is readily available for purchase as computer peripheral devices. However, considerable additional engineering and programming expertise may be required for the hardware customization and software development necessary to combine scanners, computers, optical media, video displays, printers, and other components into an effective document storage and retrieval system. The types of optical media used for electronic records storage, include:

- Write once optical disks (Write-Once-Read-Many/WORM).
- Rewritable optical disks.
- Read only optical disks (CD-ROM).
- Optical cards (laser cards).
- Optical tape.





Legal Issues

Legal standards for the acceptability of records as evidence, in formats other than paper, have been slow to evolve in response to the new technologies of the 20th century. State and federal legislation providing for the admissibility of microfilm as evidence developed gradually. Paper copies of microfilmed records have become generally accepted as admissible if microfilm was produced according to accepted standards and procedures.

The use of automated information systems is a much newer recordkeeping process than maintaining records on paper or microfilm and there is less case law to clarify how electronic records will be handled by the court. In general, the *Texas Rules of Court* allow for the evidentiary use of electronic records, as the definitions of Rule 1001 include writings and recordings set down by "magnetic impulse, mechanical or electronic recording, or other form of data compilation." Each judge may, however, dismiss evidence on the basis of the court's independent evaluation. The court must believe that records admitted before it are "trustworthy"; that is, they must clearly and accurately relate the facts as originally presented or in summary form.

In contrast to traditional paper records, electronic records have systemic vulnerabilities and additional efforts must be taken to assure the court of their trustworthiness. For automated information systems, attention to the following items will enhance record trustworthiness:

- Equipment and software reliability.
- Preparing printouts on a regular schedule.
- Records retention schedule.
- Disposition log.

To further support the admissibility of electronic records, the Texas Legislature enacted Texas Government Code §441.189, effective September 1, 1997. The new law

provides that any state record may be created or stored electronically in accordance with standards and procedures adopted as administrative rules of the Texas State Library and Archives Commission (13 TAC §§6.91-6.99). If records are created or stored electronically in accordance with the standards, then certified output from electronically digitized images or other data compilations are considered original records and shall be accepted as such by any court or administrative agency of the state.



The new law applies only to records created on September 1, 1997 and later. Although the new law is a major step forward in the admissibility of electronic records, questions may still arise in court concerning admissibility; for example, were the records actually created in accordance with the standards and procedures of the Texas State Library and Archives Commission? Consequently, other considerations may have an impact on the trustworthiness and admissibility of electronic records.

Equipment and software reliability—Since the content of a record may change if the equipment is not working properly, an organization may be required to present evidence that its equipment was operating reliably on the day the computer record was prepared. A computer operations log indicating the absence of any malfunctions is generally adequate.

Errors in computer records can also result from errors in computer programs. An organization may be required to present evidence related to the development and testing of programs. Programs are often examined by an expert witness to determine accuracy or reliability. An organization may be required to present the specific version of the computer program used to process the data being entered into evidence. A different version of the program may be considered if it is the only one available, but the absence of the exact version may raise questions on the trustworthiness of the computer records.

Preparing printouts—Computer printouts prepared in the ordinary course of business activity are perceived to have higher trustworthiness than similar computer



printouts prepared for trial. The acceptability of printouts is improved if the organization can provide an adequate audit trail to document data integrity even though there is a time lag before the computer printout is made.

Records retention schedule—An approved retention schedule can have an important impact on court proceedings because the schedule establishes a retention period and specified disposition time for the electronic records. Although an approved retention schedule for a record requested does not guarantee the court's acceptance of it, the fact that a record is scheduled helps meet the requirement of a record being created as a "regular practice" of the agency.

Courts generally accept the defense that records have been disposed of under an approved records retention schedule. The Texas State Library and Archives Commission has adopted rules for the scheduling of state records (13 TAC §§6.1-6.10). One requirement is that a state agency document the destruction of records under its approved schedule. This documentation can be an especially effective defense because it proves that records have been destroyed in the normal course of business and in compliance with the retention period specified on the approved schedule.

Final Disposition of Records

Final disposition is the last state in the life cycle of records, when they no longer serve a useful purpose for agency business. At this point the records are either destroyed or transferred to the Archives and Information Services Division of the Texas State Library for preservation as archival state records.

Records destruction—The objective of records destruction is to remove the record from possible use after it has become obsolete and to ensure that sensitive or confidential information does not become public. Because destroyed records cannot be recalled, extra care should be taken before records destruction. All state, local, and federal statutory regulations must be satisfied.

Final disposition of state records must be according to an approved “Records Retention Schedule” (Form SLR 105) or an approved “Request for Authority to Dispose of State Records” (Form RMD 102). See “Final Disposition” (Part IX, *Texas State Records Management Manual*) for additional discussion of the general procedures relating to the destruction of state records. As previously mentioned, agencies must also maintain destruction documentation to demonstrate compliance with approved records retention requirements.

NOTE: All of the destruction procedures described apply to the record copy. Convenience or reference copies should be disposed of as soon as they are no longer needed and must be disposed of by the time the record copy is destroyed. Convenience copies cannot be kept longer than the record copies.

Archival preservation—When the retention schedule is developed, electronic records having historical importance to the State of Texas should be identified. The final disposition of the archival state records must be coordinated with the State Archivist. As stated in the state retention schedule rules (13 TAC §6.8) electronic records must be transferred to the State Archives as hard copy or microform. See “Final Disposition” (Part IX, *Texas State Records Management Manual*) for guidelines concerning the disposition of state archival records.

Procedures for purging files—Written procedures should be developed for the purging and disposition of records after the retention period is complete. For electronic records, procedures need to include purging of records by personal computer users as well as the data processing department. Depending on the volume of records and the staffing situation of the agency, purging of files can be done on a monthly, quarterly, semi-annual, or annual basis.

Responsibility for approving disposition—Written procedures should verify agency policies for final disposition of records. If the agency has an approved “Records Retention Schedule” (Form SLR 105), disposition of all the records series as listed is authorized by the State Auditor’s Office and the Director and Librarian,





Texas State Library. This approval is verified on the "Certification and Approval" (SLR 105C) form, which has the required signatures.

If the records series is not listed on the approved retention schedule, or the agency does not have an approved retention schedule, the agency must use a "Request for Authority to Dispose of State Records" (RMD 102) form for permission to dispose of that records series. A records series can also be added to the schedule for approval through an amendment process. The details of the process to develop and update the agency records retention schedule are discussed in "Records Scheduling," (Part II, *Texas State Records Management Manual*.)

Disposition of original records on paper or microfilm after conversion to electronic format—An agency that wants to dispose of original paper records or microfilm after converting them to electronic format may do so if its approved records retention schedule lists the records series and shows the conversion in format from paper or microfilm to electronic media.

An agency that does not have an approved retention schedule or its approved retention schedule does not show the format change must obtain permission for the destruction of paper or microfilm records converted to electronic media through use of the "Request for Authority to Dispose of State Records" (Form RMD 102). Approval of the RMD 102 by the Director and Librarian of the Texas State Library does not grant continuing authorization to dispose of the records series listed on the form, but only for the dates or other parameters shown on the form for the records series. If, at a later date, the agency wishes to dispose of additional portions of the records series, another RMD 102 must be submitted for approval.

It is in the best interests of a state agency that routinely converts a records series from paper or microfilm to electronic media to indicate the conversion on its records retention schedule or an amendment to its schedule. If approved, the schedule confers continuing authority to dispose of the paper or microfilm records.

Destruction of Electronic Records

Electronic records are usually stored on erasable, reusable, and relatively expensive media, which are easy to revise and update, but that are also relatively fragile. For these reasons, those electronic records that are to be disposed of rather than transferred to the State Archives should be destroyed as soon as possible after the expiration of their retention periods.

Magnetic media that contain sensitive or confidential electronic records should not be discarded in regular waste containers. One method of disposition is degaussing, a method of electromagnetic erasure, although reliability of the erasure depends on the time exposed to the magnetic field and the strength of the magnetic field. The media can then be reused, or reformatted and reused, or rendered useless by shredding/disintegration. Digital shredding can be accomplished by a utility that writes binary 0's or 1's throughout the space the document occupied on the electronic medium. Data scrambling programs are also available as a means of making the file's data permanently unavailable.

These specific precautions are required for confidential information because many personal computer operating systems do not actually erase the entire file when files are "deleted." They simply remove the file's name from the system directory. This allows the space occupied by the file to be declared available for a new file. The electronic records remain unchanged until that portion of the disk is overwritten.

Consequently, "deleted" electronic records files may be recovered by using commercially available utility programs. There is a similar problem with write-once (WORM) optical storage media if only the index pointer is removed. The records must be made unreadable or the records not ready for destruction may be copied to a new disk and the old disk then destroyed.





Why Apply Records Management?

Because of the technological characteristics of electronic records and the complexity of their use, even more thoughtful application of sound records management principles needs to be given to their creation, maintenance, and final disposition. To have an effective electronic records management program, the agency records management officer—in cooperation with the information resources manager and other administrative, professional, technical, and clerical staff—should:

- Establish the necessary program elements to manage electronic recordkeeping.
- Use the records inventory to document records in electronic recordkeeping systems.
- Make the decisions necessary for developing the agency records retention schedule.
- Organize electronic files to maximize their usefulness.
- Implement security measures to protect electronic information.
- Work with the State Archives to preserve the state's historical heritage.
- Apply the approved retention schedule and agency procedures to dispose of obsolete electronic records and free up valuable needed computer resources.

Agencies are encouraged to contact the State and Local Records Management Division with any concerns regarding the management of electronic records.

As standards for electronic recordkeeping systems and procedures for their management continue to develop, the State and Local Records Management Division will provide further information to state agencies.

Comments or complaints regarding the programs and services of the Texas State Library and Archives Commission may be addressed to:

*Director and Librarian
PO Box 12927
Austin TX 78711-2927
512-463-5460; FAX 512-463-5436*

Copies of this publication are available in alternative format on request.

Published by the Texas State Library and Archives Commission, Revised June 1998



Texas State Library and Archives Commission

State and Local Records Management Division

PO Box 12927

Austin TX 78711-2927

512-454-2705; FAX 512-323-6100

<http://www.tsl.state.tx.us/SLRM/SLRMhome.html>