Records Management Guide

Records Management Office

Records Management Officer
Jim Mousa
Building 8 Room 1207
904-620-2779

TABLE OF CONTENTS

Records Management

The starting point for an effective records management program is the identification of an organization's records and the establishment of a retention schedule. A records survey or inventory is the first step. Inventories are the basis for records retention and disposition schedules. Retention schedules reflect the length of time that records have operation, legal, fiscal or historical value. The Office of Records Management has forms for use in completing surveys or inventories and can offer advice or assistance in the process.

The Department of State by legislation is empowered to administer records management and accomplishes this by way of Florida Administrative Code Chapter 1B-24 (Appendix A)

The State of Florida issues specific retention schedules for state and local government use. The University of North Florida is subject to five specific records schedules – GS - 1 S State Government, GS -5 University and Community Colleges, GS - 4 Public Health Care Facilities and Medical Providers, GS - 2 Law Enforcement and Correctional Facilities and GS 15 Public Libraries. Even with five general schedules available the University has records that are not directly covered and so must use the information gathered from a records inventory to help set specific retention schedules where necessary. New retention schedules are approved by the Department of State.

> **Note: As retention schedules required for the University are updated routinely they are not contained within this guide. Any schedule requested can be e-mailed promptly.**

When conducting an inventory, you should identify records as series – a group or unit of related documents that are normally filed or kept together because they relate to a particular subject or function. Examples include correspondence, contracts, policies, acquisitions (requisitions & purchase orders) project files, student records, cash receipts and time & leave records.

Essential components of a records management system are identified as:

- **Record Series Title**. Normally, files are organized into record series. A record series is defined as a group of records filed together because they have similar characteristics or because they perform similar functions. It is essential that titles correspond with retention schedule titles for disposition.
- **Description**. The description of the record series identifies the record's purpose and function with regard to the agency's operation. The description indicates exactly how the record is used and why it was created. Additional information in the description might include the medium on which the record is recorded, routing path of duplicate copies, statutory requirements for creating the record, etc.
- **Inclusive Dates**. When first identifying the records retained in an office, it is important to determine the relevant date ranges to which those records pertain. This is necessary in order to ascertain if records are being kept longer than required.
- **Volume**. The volume of space required for records storage can be considerable. When the inclusive dates of a records series retained in an office far exceed the requirements specified by a retention schedule, an organization can realize significant savings when the records retained beyond the retention schedule requirements are destroyed. (See Volume Conversion on page 5)
- **Retention**. If an approved retention period already exists, this retention requirement should be noted on the inventory form. If no retention period exists for the record series, note the time period that the record series is administratively active.A good records management program within a department can provide several benefits.

  - **Space savings.** By implementing retention schedules and systematically destroying those records that are either duplicates or have already met their retention requirements, an office or department can reduce the space occupied by records up to 40%.
  - **Reduce expenditures for filing equipment.** Disposing of obsolete or duplicate records can reduce the need for additional file cabinets.
  - **Compliance with legal retention.** The management of records based on an analysis of legal, fiscal, operational, administrative, and historical requirements will reduce the risk of improper destruction of public records.
  - **Protection of vital records.** The process of establishing a records management program will in turn identify vital records for which you should develop a disaster recovery plan. Could your office/department recover from a catastrophe today?

Records Disposition

What is records disposition? It can be several things. It can be the shredding of records approved for destruction. It can be the transfer to microfilm or optical disks. It also can be the transfer of custodial responsibility to a State agency, e.g., State Archives in Tallahassee.

Most often when records disposition is mentioned it is in terms of "how do I get rid of old records?" The first step is to identify the records you wish to dispose of, what time period and how large the quantity is. (It is essential that the title of the record series on the disposition match the record series title in the retention schedules.) This information must be placed on a Records Deposition Request, signed by the area custodian and forwarded to the Office of Records Management for approval. ("Custodian" means the position holder charged with the responsibility of maintaining the office having public records, or their designee.)

The approval is currently a two working day process. Once approved a copy of the disposition is returned with instructions for disposal, certificate of disposition and labels for boxes. Those records authorized for shredded destruction will be picked up by Recycle as indicated in the instructions. Once shredding is completed Recycle will forward the signed certificate of disposition to Records Management.

For identification, inventory and disposition of records the following information will be included on container labels:

Item number – available from Records Management **Schedule number** – available from Records Management Officer **Record series title** – additional description of material may be necessary

Calculating Eligibility Dates

If the ending date for a specific record series is 7/31/97, when can these records be destroyed?

Date to Start	Add # of years	Date eligible for destruction	Counting
3 years 7/31/1997	+3	= 7/31/2000	3
fiscal years 7/1/98	+3	= 7/1/2001	
3 calendar years 1/1/1998	+3	= 1/1/2001	

Records Volume Conversion to Cubic Foot Measurements

Cassette Tapes (200) 1.0 cu. ft. Letter-size file box (12x12x10) 1.0 cu. ft
Legal-size file box (15x12x10) 1.5 cu. ft. Letter-size file box (12x24x10) 2.0 cu. ft. Letter-size, file drawer 29" 2.0 cu. ft. Legal-size, file drawer 29"
2.5 cu. ft. Letter-size, file shelf 36" 3.0 cu. ft. Legal-size, file shelf 36"
3.5 cu. ft. Magnetic Tapes (12) 1.0 cu. ft. 3 x 5 card, ten 12" rows 1.0 cu. ft. 3 x 5 card, five 25" rows 1.0 cu. ft 4 x 6 card, six 12" rows 1.0 cu. ft. 5 x 8 card, four 12" rows 1.0 cu. ft.
3.5 Disks (500) 1.0 cu. ft.

Files Management

Why Files Management?

The basic objective of a good filing system is to be able to find the record you need quickly and economically, regardless of its format.

Files management is integral to records management. Records Management is the application of systematic control to recorded information. It is a logical and practical approach to the creation, maintenance, use and disposition of records and, therefore, to the information that those records contain. Files Management applies records management principles to both paper and electronic records created and used by a single office. Files management ensures the use of information by providing that records can be retrieved when needed.

Responsibility

Each university office/department has the primary legal responsibility for the proper care and management of its records. To meet this responsibility each office should designate a records coordinator and notify the Office of Records Management so that a communications link can be established.

Filing Arrangements

There are three commonly utilized types of filing arrangements: alphabetical, numeric, and alphanumeric. Each has advantages for certain types of records and reference needs and possesses distinct patterns of arrangement and indexing. The most efficient and economical method is the one that works for your office/department and is easily understood by its users. Generally, the simplest method is the best.

Once a filing arrangement is chosen, the following determinations must be made to establish the files:

1. What the filing units are,
2. What the arrangement of filing units must be to create the system,
3. What information is placed on the guide,
4. What information is placed on the folder.

Once the proper arrangement has been selected, it is suggested that a file standards and procedures manual be established. The use of a manual by everyone working with the files will maintain the integrity of the filing system.

Alphabetical file

The most commonly used filing arrangement is the alphabetical file. It is arranged in alphabetical order with a file guide for each letter of the alphabet.

The alphabetical arrangement is commonly used for correspondence. It is estimated that 90% of all filing is the filing of correspondence, and that 90% of this follows the alphabetic arrangement of names. As long as the name is known, anyone can have direct access to the file without an index. Alphabetical filing systems are very flexible.

> **Records Management suggests that departments using the alphabetical file method start a new folder for each time period, e.g., fiscal year. This will assist you in separation into the different retention periods.**

Numeric file

In a numeric file arrangement, records are classified by number rather than name. Numeric files originate where the number is part of the record itself or where a number is added to facilitate processing and filing. When a number is part of the record, reference will often be by number. When numbers are added, reference will usually be by subject. Numeric files are usually divided into three basic types: serial number filing, used basically for fiscal records; digit filing, used in student number files, is the best method for filing and referencing extremely large file series. Numeric coding of subjects and names, in which number are assigned to replace the subject or name titles on the folders also works well.

Note: In setting up a new numeric file the use of social security numbers is restricted by Florida Statute 119.072.

Alpha-Numeric file

Alphanumeric filing is the classification of records by codes. The codes should give information about the contents of the folders. Alphanumeric filings are divided into two types: subject files and name files. Subject files follow an encyclopedic arrangement with numeric coding of records and folders. Name files are usually filed alphabetically with names arranged in sequence according to exact spelling, and are dependent on the accurate interpretation of the spoken or handwritten name.

Note: A complete Files Management handbook is available from Records Management.

Electronic Record-Keeping

The use of electronic records has expanded in recent years. Use has grown so rapidly that a new Administrative Rule (1B-26.003), "Records Management – Standards and Requirements – Electronic Record-keeping" was created by the Dept. of State (Appendix B). The rule defines electronic records as "Including numeric, graphic and textual information that may be recorded in any machine readable media form that includes, but is not limited to magnetic media, such as tapes and disks (hard or floppy) and optical disks."

Electronic records may include "data files" and "databases", machine-readable indexes, word processing files, electronic spreadsheets, electronic mail and electronic messages, as well as other text or numeric information. Electronic record keeping involves the use of a computer to create, store, retrieve, analyze, transmit or delete records.

The primary consideration when establishing record-keeping requirements for electronic records is the definition of an electronic record? Chapter 119, Florida Statutes provides a definition of "public records" and the Florida Supreme Court has rendered further interpretation. Therefore, any electronically recorded data which is: (1) made or received pursuant to law or ordinance or in connection with the transaction of official business, or (2) any material prepared in connection with official agency business that is intended to perpetuate, communicate or formalize knowledge of some type constitutes a public record.

Electronic documents are records just as much as paper documents, and their creation, maintenance and use, and disposition must be managed accordingly. The most common types of document-based electronic records are word processing files, spreadsheets, presentation graphic files and e-mail messages.

Currently, PC users are pretty much at their own discretion regarding retention and maintenance of their electronic records. Many times PC users use arbitrarily selected file names that are familiar to no one but them. This lack of organization can easily lead to lost files or worse the user may leave the University and then no one can access what may be a critical record.

Using an average of two files created a work day and 260 work days a year you can quickly see the quantity of records created and stored on desk top PC's at the University. The development of an office/department filing procedure manual or guide shall include a section for electronic records.

All systems require that new files (documents) be given names in order for the computer system to save them. The document name usually consists of a drive identity, a directory, subdirectories, the document label, and a software extension. An example might be F:/Administration/Budget/1998/Final.doc with each part being identified as follows.

F = drive
Administration = directory
Budget = sub-directory
1998 = sub-subdirectory
Final = file name
doc = software extension

Offices/departments should develop standard naming conventions for their electronic records. A combination of subdirectory and file naming conventions should capture enough information to find, identify and access each electronic document. There are many advantages to standardizing the naming conventions for electronic documents. Standardized file names allow offices to:

- access files easily and rapidly,
- reduce redundancy of files,
- avoid loss of information
- find the latest draft or the desired version of a document,
- name files quickly and easily,
- share files easily.

Naming conventions should be based on factors such as business processes, retention requirements, location of users and retrieval requirements. If the office already has an established filing system for its manual files, directories and subdirectories can be established using categories that are similar to the major file classifications of the manual files.

Careful consideration should be given to the development of convenient categories for filing and retrieval of electronic documents.

An office/department may classify its records first by:

- reviewing physical records file arrangements,
- creating primary categories that are functional, not department-based,
- creating secondary categories that reflect the office process,
- developing an index.

In most cases, the record status of electronic data should be apparent. When evaluating the occasional doubtful situation, the safest course is to regard it as a record and proceed accordingly. Records Management staff can offer advice about the record status of electronic information, but the final administrative decision rests with the record custodian.

The Florida Department of State, Bureau of Archives and Records Management has provided some suggested directories and sub-directories that might be used to organize and control information maintained on PCs.
Each area needs to put in place a set of directories that will support the unit's mission and control electronic records in accordance with Florida Statutes. Below are some of the suggested directories:

. o ADMINISTRATIVE REGULATIONS – This directory is for posting and maintaining policies, procedural directives and manuals developed by a unit or the agency to govern its internal management.
. o ANNOUNCEMENT – This is a common directory used for making general agency announcements, changes in policy, position openings, meeting announcements, etc.
. o ADMINISTRATIVE CORRESPONDENCE – Correspondence related to the administration of an agency or division concerning the coordination of programs, agency policy, and non-routine actions and responsibilities.
. o ADMINISTRATIVE SUPPORT – Consists of office/dept/division files documenting the substantive actions of directors/department heads, assistants and associates.
. o GENERAL CORRESPONDENCE FILES – This file consists of general, day-to-day operating information with private sector individuals and other governmental agency personnel that relates to non-policy development matters.
. o RECORDS MANAGEMENT -- This directory contains documents related to an office/dept/division's records management program.

Understanding the distinction between a "master copy", "duplicate" and "intermediate" record can conserve time and effort. These definitions of master and duplicate are contained in Chapter 1B-24 Florida Administrative Code, and intermediate in Attorney General Opinion 85-87 (Appendix C). The reduction or elimination of copies is a vital goal in all automation planning. The convenience of copiers and computers has made the determination of what and when a document is a "duplicate" or "intermediate" record difficult. However, as a general rule most copies can be destroyed whenever it is convenient, provided a "record (master) copy" is maintained. The master copy is the legal document, the document that is the proof that your office/department/division performed a specific function in the proper manner.

The "master copy" is that document filed with the **initiator** and not the original. Generally, the unit that initiates a letter, memo or policy files a copy. This copy is considered the master. This is the copy that validates the content of your correspondence. Office/dept/division procedures need to define a master and specify its location and content. The records custodian determines the master file location. This is especially important when this copy is maintained on a magnetic medium or generated from a database, particularly if no paper master is created.

"Record (Master) Copy" means public records specifically designated by the custodian as the official record.

"Duplicate (or Convenience) Records" means reproductions of record (master) copies, prepared simultaneously or separately, that are designated as not being the official copy.

"Intermediate Records" (Processing Files) are temporary records used to create, correct, reorganize, update, or derive output from master data files. Intermediate records are precursors of public records, and are not, in themselves, public records that must be retained. Intermediate records only exist provided a final product is subsequently generated which perpetuates, communicates, or formalizes knowledge of some type. In the event this precursors fails to create a Copy of Record, then the precursor becomes a Copy of Record.

It is essential that the custodian of electronic records understand that access to electronic public records is their responsibility. Thus, the custodian must maintain software and systems capable of accessing said electronic records.

The University backs up the global drives but this does not include individual pc's "C" drives or "My Documents" thus the office/department should initiate a method of backup and storage.

WEB Sites

Many do not realize that an established web page within the context of University business is a public document. The process of updating or adding to a web page alters or destroys an existing public record. Documents are removed from web sites for many reasons, including:

- They no longer reflect current policy.
- The information in them has been superseded.
- Hard copies have been generated for retention/preservation.
- Official copies exist elsewhere.

Those with responsibility of changing, updating or adding to web pages should create a file for purpose of creating an archival record of web pages. Such a process would assist in meeting public records retention requirements.

Disposition of Electronic Records

The disposition of electronic records is processed in the same manner as a hard copy or paper record. The initiator or holder of the copy of record must insure that the disposition of electronic records is authorized and recorded.

Electronic Mail

Electronic mail is the electronic transfer of information typically in the form of electronic messages, memoranda and attached document from a sending party to one or more receiving parties by means of an intermediate telecommunications system. Electronic mail that is created or received by any organization in connection with official business is a **record** that is subject to **records management and retention laws and regulations** as stated in AGO **81**-DS-L (Appendix D)**.**

In order to properly manage e-mail systems and their contents, it is necessary to acknowledge and understand the following principles and requirements:

1) Electronic mail messages are public records when they are created or received in the transaction of official business and retained as evidence of official policies, actions, decisions, or transaction. Electronic mail messages that are kept because they contain valuable informational content are also records. Electronic mail messages that constitute public records must be identified, accessible, and retained just like records in other formats.
2) Electronic mail messages are not subject to the provision of the Public Records Act, Chapter 119, Florida Statutes when they consist of un-circulated materials and are merely preliminary or precursors to future documents, and that are not in and of themselves intended to serve as final evidence of the knowledge to be recorded.
3) Internal and external personal communications or announcements of a non-business nature and personal notes intended for ones personal use is a question mark. Is this a record subject to retention and public inspection? Recently Florida Courts have said personnel e-mail fall outside the definition of public records because they are not connected to official business.
4) Electronic mail records are to be readily available and accessible to all authorized users when they are needed and are to be in a useable format. The identity, purpose, and location of records should be predictable, consistent and reliable; methods for access and retrieval should be simple and well defined; and records management practices should be incorporated into daily business activities.

5) Each organization should define proper use of electronic mail systems and set limits on personal use. 6) Public records that are transmitted and received through electronic mail systems should be organized and stored in a filing system or repository. 7) Each organization should ensure that adequate training in record-keeping requirements is provided for users of electronic mail systems.

Note: Be aware that all e-mail sent or received on the University systems will be retained in the routine backup of electronic files.

All users of university computers are responsible for compliance with the Policies, Procedures and Guidelines issued by Information Technology Services. These can be found at **Records Management** and include the policy on Electronic mail; Computer and Network Use Policy and Responsible Use Policy.

Social Security Number

Wherever possible, the use of social security numbers should be minimized and action must be taken to protect the confidentiality of social security numbers as required by federal and state law. University employees should be aware of the following two state statutes:

- 119.0721(5)1 On or after October 1, 2002, any person preparing or filing a document for recordation in the official records may not include a social security number in such document, unless required by law.

- 119.0721(8) An agency shall not collect an individual's social security number unless authorized by law to do so or unless the collection of the social security number is otherwise imperative for the performance of that agency's duties and responsibilities as prescribed by law. Social security numbers collected by an agency must be relevant to the purpose for which collected and shall not be collected until and unless the need for social security numbers has been clearly documented. An agency that collects social security numbers shall also segregate that number on a separate page from the rest of the record, or as otherwise appropriate, in order that the social security number (can) be more easily redacted, if required, pursuant to a public records request. An agency collecting a person's social security number shall, upon that person's request, at the time of or prior to the actual collection of the social security number by that agency, provide that person with a statement of the purpose or purposes for which the social security number is being collected and used. Social security numbers collected by an agency shall not be used by that agency for any purpose other than the purpose stated. Social security numbers collected by an agency prior to May 13, 2002, shall be reviewed for compliance with this subsection. If the collection of a social security number prior to May 13, 2002, is found to be unwarranted, the agency shall immediately discontinue the collection of social security numbers for that purpose.

Public Records

Florida Statutes Chapter 119 defines public records in a broad and all-inclusive language.

> **"Public records" include all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.**

Florida's Public Records Law provides for citizens to have an unparalleled access to the records of government. Chapter 119.07(1)(a) states that:

> **Every person who has custody of a public record shall permit the record to be inspected and examined by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record or his/her designee.**

Who can request public records.

> **Florida's Public Records Law requires that "all state, county, municipal records shall be open for personal inspection by any person." [s. 119.01(1), F.S.] "Person" is defined by statute to include: individuals; firms; associations; joint adventures; partnerships; estates; trusts; business trusts; corporations; etc. [s.119.01(3), F.S.] A requestor does not have to be a Florida resident.**

Not every record generated by the University is open for inspection. Section 119.07(3) exempts certain records from public inspection. Questions concerning the Florida Public Records Law should be referred to the Office of the General Counsel.

When a public record contains both exempt and nonexempt information, an agency is required by law to delete – redact – that which is exempt, and to provide access to the remainder. Thus, a public records request cannot be denied based on the fact that the requested record contains exempt information. Additionally, if an agency denies a request claiming that the record or information is exempt from disclosure, the agency must state the basis for the denial in writing, and include the exact statutory citation for the exemption, if so requested. [s. 119.07(2), F. S.]

What Is A Vital Record?

A Vital Record is recorded information, regardless of format (i.e., paper, photo, database, magnetic tape), that must be protected in the event of an emergency or disaster because of severe consequences to the office and the University of North Florida if the record is lost or destroyed.

Vital records are records that will be needed in anywhere from a few minutes to 24 hours after a disaster to get an office up and running again. They are records that, if lost or destroyed, would be both costly and time consuming to recreate – if they can be recreated at all. They can be active (currently used by the office) or inactive (in storage).

Vital Records are:

- Essential to the function and mission of the University.
- Essential for the continuous operation or reconstruction of any University owned buildings.
- Necessary to establish or protect the legal or financial position of the University.
- Necessary to protect and ensure the rights and interests of the employees and clients of the University.

Tips for identifying the records that may be vital are outlined in How To Identify a Vital Record. Only a small percentage of the records will be vital; most will fall into one of the following three categories:

Essential Records – These are records that will be needed within 72 hours after an emergency and, although it may be costly and difficult, CAN be reconstructed or replaced from other sources.

Useful Records – These are records that can be easily replaced. The time and cost of reproducing or accessing these records would be minimal because of the ready availability of these records at other locations.

Non-Essential Records – These are records that are of little or no value to the office and probably should never have been retained. Examples would be stores catalogs, brochures, extra forms, etc.

Individual offices need to complete an analysis of their records in order to identify under which of the categories the records will fall.

Listed below are University records that may be classified in the areas of vital, essential and A record is either vital or it

Vital Records

Administration Records for Grants/Contracts
Accounts Payable/Receivable
Consent Forms – Adult and Minor
Payrolls
Insurance policy information
Patents and Trademarks
Transcripts
Bid Documents
Capital Assets
Budget Records
Human Resource Records
Master Plan
Application for Internal Research Support--Awarded
Purchasing Leases and Contracts
Endowment Fund Records
General Ledgers
Committee Minutes
Research Data
Blueprints of Facilities
Police Records
Organization Charts and Listings
Deeds for University owned property
Student Records

Essential Records

Accreditation Documentation
Billing Source Documents
Grade Appeals
Annual/Monthly/Quarterly Reports
Current Calendars, Appointment Books, & Daily Schedules
Grievance Files

is not vital. A guideline is the question "what records are essential to emergency operations of this office/department?" What records are essential to re-establishing normal operations of the agency after an emergency ceases?

Why Are Vital Records So Important?

Identifying and protecting Vital Records provides a route to re-establish normal operations in the office soon, if not immediately, after a disaster. By realizing the importance of records for continuing the office functions and arranging for protection of these records, valuable time and resources will be saved after an emergency. The ability to concentrate on restoring operations rather than finding necessary information or spending money and time on restoring unnecessary records.

The identification and protection of Vital Records is crucial:

- Minimize the disruption of normal business operations after an emergency.
- Minimize the economic impact of the disruption.
- Provide for rapid and smooth restoration of services.
- Comply with legal and regulatory requirements.
- Recover and/or salvage office vital records and assets (i.e., equipment) rather than using time to recover unnecessary information.

Regardless of the damage received due to a disaster and the resulting problems experienced in reestablishing normal operations, other offices may have immediate need of the records/functions your office provides. That makes Vital Records in one office important not only to it but also to the University community.

Note: The Florida Administrative Code section 6C9-1.012(8)(b) requires record custodians maintain security and integrity of records whether stored in the offices or in off-site areas.

Some federal guidelines may apply to departments/offices that receive funding in the form of federal grants. When an office is audited by a federal agency that has issued it a grant, failure to provide records requested because of a disaster is not considered an adequate response to an audit request.

How To Identify A Vital Record?

Identifying the Vital Records in an office is a critical task. It needs to be done immediately so that arrangements for protection can be made prior to a disaster. By applying the steps listed below, each office will be able to identify the records that may be necessary to continue office functions after a disaster.

Step 1: Identify the key functions or responsibilities based on the following criteria:

- Operational – Any functions that are vital to the operation and continuation of the office or the University.
- Legal – Any functions that provide proof of the University's legal stand on an issue.
- Emergency – Any functions that are needed during an emergency, e.g., telecommunications, utilities or first aid.
- Fiscal – Any functions that prove the University's financial standings, e.g., accounts receivable or general ledgers.

Tools to help identify the unique functions may include:

- Functional/Organizational charts. If these exist, they are a good place to start as they provide a comprehensive list of normal functions.
- Records Retention Schedules. These retention schedules provide a list of all records that may be unique.
- Departmental Records Inventory. Inventories will identify unique records for the office or department and may provide a direction for copies of records.
- Crisis Management Plan. While the plan is geared towards emergency personnel (i.e., police, fire department, facility operations), it will help identify what office is responsible for specific functions in the event of an emergency.

Step 2: Once the key functions/responsibilities are identified, answering the following questions will help determine Vital Records.

- What function cannot be managed if this record is destroyed?
- How critical is the inability to perform this function?
- What will be the consequences to the University if these records are lost?
- Will any client, employee, or student of the University suffer loss of rights or be severely inconvenienced if these records are lost?
- If these records have to be reconstructed, what will the cost be in terms of time, money and labor?
- Will the information in these records have to be reconstructed or retrieved in a matter of hours, days, or weeks?
- Can these records be replaced from another source?
- Are these records on computer, disc or microfilm?
- Is the format easily accessible after an emergency?

Other considerations to determine if records are vital:

- Uniqueness of the record.
- Relationship of one record to another.
- The type of information needed during and following an emergency.

How To Protect And Store Vital Records?

- o **How to Protect Vital Records**
- o **How to Store Vital Records**

How to Protect Vital Records

After identification of Vital Records, a protection method that best suits the record format must be provided. The protection method will be based on several factors, including:

- Cost and effectiveness of protection.
- Equipment necessary to enforce the protection method.
- How vital the record is.
- Format of the record.
- Access and retrieval needs.
- Type of hazard the record faces.

Vital Records should be stored in a format that will last as long as the records are needed. If a Vital Record is in a format only readable by specific equipment (e.g., microfilm reader, computers), procedures for accessing/obtaining the equipment must be arranged. **If a Vital Record is in electronic format, then the hardware or software used to create the record also needs to be protected or arrangements made to obtain compatible equipment.**

The main protection method for Vital Records is through **Duplication/Dispersal** of records. This entails the physical duplication of information and the transfer/dispersal of these duplicates to an on/off site storage location.

The **benefits** of duplication/dispersal:

- Minimal chance that the primary copy and all distributed copies will be destroyed.
- It is cost efficient.
- It is easy to do and usually done in the normal course of business.

The **drawbacks** to duplication/dispersal are:

- The volume (e.g., number of pages or number of copies needed) of the records may cause this method to become burdensome over time.
- The distribution of additional copies of information on paper is a poor records management practice. In cases where several offices have the same record, responsibility for the original is not always clear. Offices that do not have responsibility for the copy of record tend to keep their copy too long.

There are two ways of achieving duplication/dispersal:

- **Natural/built in:** The information is routinely distributed to other departments, offices, or individuals. This is the least expensive form of protection since it often occurs in the normal course of business, usually without offices being consciously aware of it. (This is not a protection if distribution is contained within a single location.)
- **Reproduction:** This represents the decision to duplicate or transfer the record onto a different format specifically for its protection. Microforms, magnetic media or optical imaging are the most common forms of reproduction.

o Microform (film, fiche) requires a specialized reader and printer to access information. It does not matter which format is used, the process is the same for both. **Working and security copies should be created for either type and stored in different locations.**

- Working copy – The working copy is produced on Diazo film that does not scratch as easily as the Silver film. It is very durable and should be used for everyday reference purposes.

- Security Film – The security copy is produced on Silver Halide film. This is a master copy and should not be used in a microfilm reader. It should only be used to generate more working copies (Diazo copy) of the film.

The best way to store the security copy is in an environmentally controlled secure storage area. It could be financially beneficial for multiple offices or departments to join together to have access to a secure storage area. If the office does not have access to such an area, the Silver film should be stored in a dust free area, in its protective case. However, never store the Silver film and the Diazo copy in the same area (e.g., box, cabinet, filing drawer) because the out-gassing of the Diazo copy will degrade the Silver film, making it unreadable and useless for the production of additional copies.

Advantages of microforms: They are very inexpensive to duplicate. They are compact and easy to store/handle/move. They have proven to last over 100 years and have a life expectancy of approximately
500 years

Microforms do have an inherent disadvantage: The initial cost of preparation and the actual filming of records can be high.

o Magnetic tapes/electronic media/optical images are acceptable for the protection of Vital Records having a retention period of up to ten years. Since magnetic tapes have limited stability, special handling is needed to ensure the preservation of electronic records. Media stability refers to the period of time during which the media can be used for reliable recording or playback of the information. The useful life of magnetic tapes is estimated to be 10 years while optical disks claim to have a life span of 100 years. Yearly review of the tapes or disks to ensure the information is readable and to migrate the information to new systems is recommended.

Criteria for using magnetic media:

- Data must be superseded or updated so frequently that it precludes the economical use of microfilm or paper. If the information is updated everyday and making an electronic copy is easier or more cost effective than photocopy or microfilm, using magnetic media for Vital Records storage could be a viable option.
- Continued access to the equipment and software needed to retrieve, read, and reproduce the information is required.
- The ability to migrate all information to new media every time hardware or software is upgraded is a necessity.
- The information is most easily read in an electronic format.

Magnetic media have some inherent disadvantages when used for security records:

- They can easily be erased, or data can be lost, due to contact with magnetic fields or through improper storage conditions.
- Retrieval of information from magnetic media is all but impossible if you do Not have the equipment or software for the media.
- Cost of maintaining necessary equipment and software.
- Cost of continued migration of data to new media.
- Limited media stability.

If magnetic media is selected as the security storage media, the programs, machine instructions, system documentation, and other items required to access the records become Vital Records and must be protected accordingly.

o Optical imaging is a process used for paper, microfilm, photograph and photocopied records. They are reproduced (by a scanner) and turned into a digital image file. The imaging process can create a photographic image of the record, or optical character recognition (OCR). OCR is a process that the scanner and the software read the record and interpret the letters on the page, thereby reproducing the content of the record (but not a photographic image) into the digital file. Both imaging processes are acceptable, as long as they produce an accurate reproduction of the record.

As these records can be altered, agencies must document how they created the digital image and authenticate or certify the image. The process of image creation will be analyzed when a court of law attempts to authenticate the record.

The advantages of using optical imaging:

- Computer systems that use optical disks can have very fast processing speeds
- Computers can allow multiple users simultaneous access
- Optical Imaging disk can be set not to allow alteration of data
- Ease of electronic data collection

The disadvantages of using optical imaging:

- Indexing of images will allow simple search and retrieval of information, but good indexing is not guaranteed.
- Optical disks are not an ideal storage medium for long-term and archival retention of electronic records. Optical disk (in many cases) can only be read by the system that created the disk.
- Any electronic media used to store records with long-term or archival value will need to be continuously migrated and/or refreshed using future technology.
- Software and hardware manufacturers improve their products and put new versions on the market every six months or so. As a result hardware and software often become obsolete, with no guarantee that products will be compatible. When using an optical image system the following should be strongly observed.

Maintain non-permanent records with an established retention of no more than 10 years in an optical disk system and dispose of the originals provided they:

- Maintain security copies of the disks and indexes in off-site storage.
- • Either migrate or convert both the working & security copies of the disks and indexes if optical systems are upgraded or changed in a way that prevents access to the contents of the disks created by the old system or recopy to new disks every eight to nine years, whichever occurs first.
- Sample both the working and security copies of the disks and indexes at least once a year to make sure the data is readable and recopy to new disk immediately if any loss of information is detected.
- Obtain an authorization for disposal/transfer from the Office of Records Management prior to such actions.

The Florida Department of State, Division of Library and Information Services provides a central microfilming service for the benefit of offices/departments that use microfilming for storage of records with long term retention requirements. The Bureau offers planning and evaluation of microfilm projects for small or one-time applications as well as large on-going projects. Additional information for micrographics is available from the Division of Library and Information Services at 904-487-2180 or SunCom 277-2180.

When considering the use of a commercial source for micro-graphics insure that the process is equal to or better than that of Florida Administration Code 1B-26.0021.

How To Store Vital Records

After determining what method will be used to protect Vital Records, determining where and how to store the records is crucial. The location you chose will need to be accessible within seconds to 24 hours after a disaster. Vital Records can be stored on-site, off-site, or in specialized equipment.

On-Site Storage

On-site storage means storing Vital Records in the same vicinity as your office, such as in a closet or storage area in the building. The drawback to choosing on-site storage is that if a major disaster strikes the entire building or damages to it may be beyond repair, there will be little chance of retrieving your Vital Records.

When storing Vital Records in the same location that the office occupies is necessary, take precautions to prevent a disaster from spreading to the areas where the Vital Records are stored. This could range from installing fire doors and walls, to following basic best practices to protect the records. Best practices range from actual physical location to working conditions within the storage area.

The following should be taken into consideration and resolved for each office that has Vital Records in their active files:

- Does the storage area have ventilation? Does it have proper temperature and humidity controls?
- Are there electromagnetic fields nearby that could damage computer tapes or disks?
- What security measures are in place to stop unauthorized access to the area?
- Is the building itself secured against fire, flood and other disasters?
- Is the equipment used for storage adequately safe from disasters and sabotage?
- Is the storing of the only copy of a Vital Record safer on-site or off-site?

Once the on-site storage location has been chosen, the following concerns should be addressed:

- Check for potential fire, water or sewer hazards. Any corrections or repairs should be made immediately (leaking overhead pipes may cause a disaster). Records should never be stored directly under any type of pipes.
- Staff members should know the location of the vital records and access to materials should be restricted to authorized personnel.
- Aisles and doorways should be kept clear at all times.
- Inactive records should be reviewed semi-annually to determine off-site storages or disposition requests.
- Staff members should know the location of all ABC fire extinguishers.

Ground floor areas should be used for storage as a last resort since they are most susceptible to water and sewer damage.

Off-Site Storage

Off-site storage means storing the records away from the offices, in another building or out of the geographical area. There are several options for off-site storage, including hot sites, cold sites and records centers.

Both Hot and cold sites are affiliated with offices that rely heavily on the recovery or availability of databases or electronic records for continuance of their normal operations. For simplicity we will apply the concept of a hot-site to all media formats.

- Hot site – An area identified prior to an emergency/disaster as the meeting place where the office staff will attempt to get organized to continue daily operation. This method of protection can be costly and is best used by offices that will require computer systems to be up and running immediately after a disaster, or by offices with the responsibility for organizing and running recovery procedures (e.g., police, physical plant, computing and communications).
- Cold site – A cold site is an off-site location used expressly for records storage. Site is not an operational site. Using a cold-site for the storage of Vital Records, the cost of duplicating and delivering/retrieving to and from the site must be considered in the cost analysis.

Specialized Equipment

The use of Specialized Equipment, such as vaults, fire-resistant cabinets and/or fire-resistant safes, represents another type of on-site storage. While this equipment may provide some initial protection against fire damage, it may not be immune to water damage. Fire-resistant equipment is often used as a last resort when there is very little office space or no storage areas available to hold duplicated Vital Records.

Disadvantages of specialized equipment include:

- The possibility of spontaneous combustion when a drawer is opened after a fire, the result of oxygen being released back into the drawer's atmosphere.
- Inadequate protection from extreme temperatures. If the fire is hot enough, the paper records will burn in the drawer.
- The high cost of specialized equipment.
- The susceptibility of specialized equipment to water damage.
- Materials used in construction will make specialized equipment heavy and burdensome, which can be a hazard after a fire because of increased weight from water gain.

If specialized equipment is going to be used it should be designed specifically for the type of record medium it contains and used exclusively for Vital Records.

Satisfactory fire-resistant cabinets/vaults are rated according to the maximum number of hours they can be exposed to fire and maximum temperature while still protecting the contents. For example, a rating of UL 150-3 means that this piece of equipment has an Underwriter's Laboratory Class 150 rating with 3 hours of protection from fire damage. Vendor catalogs will give the specifications and equipment costs according to level of resistance. However, keep in mind that the "hours of protection" will decrease as the temperature of the fire increases.

Steps For Offices to Follow

The one thing to remember when dealing with Vital Records is that every record cannot be saved. The following steps can:

- Protect some records against disaster.
- Lessen the damage caused by a disaster.
- Identify those records that merit restoration if they are damaged.

Each department or office is responsible for identifying and protecting Vital Records.

Responsibility – Each office/department should identify the individual or individuals responsible for identifying vital functions and Vital Records. Responsibility for records identification can lie with one person or with a team. If a team will be established, personnel included can be from areas within the office or from outside of the office. The individual or team should also be responsible for arranging for the protection of the Vital Records and organizing recovery efforts, etc.

Identification – When identifying Vital Records, it is necessary to identify the main responsibilities or functions. Determine which records the office is unable to operate without if destroyed and how critical is this inability. Additionally, determine those responsibilities unique to the office and that protect the interests of clients, students or staff of the University and then identify what records are created or needed to complete these responsibilities. These records represent a preliminary listing of Vital Records.

It will be necessary to speak with people who are actually responsible for the functions identified in order to gain an insight into the daily use of the records. The people that work with these records on a daily basis will be able to prioritize their importance and identify those that are the most vital. For computer systems, talk not only to system administrators, but also to the data entry personnel and individuals who use the system most often.

Once Vital Records have been identified, a list should be maintained that identifies their location and if any method is being used to protect them. The person responsible for Vital Records should continually update this list and make it available to the rest of the office.

Risk Assessment – A risk assessment will assist in determining the appropriate protection method to use for Vital Records. Risk assessments identify the potential hazards a record faces as well as how the records can be damaged by those hazards. Hazards can range from a natural disaster to spilled coffee, computer crashes to unlawful access. While this is an exercise in probability, it will narrow the scope of protection methods and allow for some early disaster preparedness.

There are three basic steps to completing a risk assessment:

- Identify the risks your office may encounter
- Determine what level of impact the risk will have
- Calculate the probability of that risk happening

Identify the five or six most important risks to a particular office/department.

After the top risk has been identified, list the individuals who can help with recovery from that risk. This could include maintenance staff, campus police, systems staff, etc. If no one on campus has the necessary skills, consider setting up an agreement with a private contractor (See Disaster Management, page 30).

Vital Records

There are three categories of disasters:

Administration Records for Grants/Contracts
Accounts Payable/Receivable
Consent Forms – Adult and Minor
Payrolls
Insurance policy information
Patents and Trademarks
Transcripts
Bid Documents
Capital Assets
Budget Records
Human Resource Records
Master Plan
Application for Internal Research Support-Awarded
Purchasing Leases and Contracts
Endowment Fund Records
General Ledgers
Committee Minutes
Research Data
Blueprints of Facilities
Police Records
Organization Charts and Listings
Deeds for University owned property
Student Records

Essential Records

Accreditation Documentation
Billing Source Documents
Grade Appeals
Annual/Monthly/Quarterly Reports
Current Calendars, Appointment Books, & Daily Schedules
Grievance Files

Useful Records

Bank Records
Equipment Maintenance/Service Reports
Subject files
Correspondence
Registrar's Statistical Reports – Copies

Natural Disasters	**Technical Disasters**	**Human Disaster**
Flooding	Power failure	Data entry
Fire	HVAC failure	Improper handling of sensitive data
Wind damage	Failure of CPU	Unauthorized access
Ice storm	Software failure	Destruction of data
Epidemic	Electromagnetic Interference	Robbery/theft/burglary

Protection and Prevention – Once potential risks have been identified, determine a protection method for Vital Records. Depending on an office's functions, some of the vital records identified may be protected through natural duplication or reproduction. Arrangements for off-site or on-site storage should be made and the location of copies should be indicated on a Vital Records List.

Prevention measures can be as simple as not using water-soluble ink on Vital Records or as complex as establishing scheduled back-ups of computer systems or sending Vital Records to off-campus storage sites. The identification and protection of Vital Records is only one part of prevention. It is also necessary to be sure that identified steps are taken to help increase the probability that records will be available after an emergency.

Recovery – After an emergency there is always the chance that records will be damaged in some way. Some short tips for stabilizing damaged records until assistance can be gotten.

Due to the differences between various media types, recovery efforts will vary from office to office. But there are a few basic rules that all offices need to follow after a disaster:

- **Do not use fans in rooms that have water-damaged records.**
- **Keep the temperature as cold as possible in rooms that have water-damaged records.**
- **Keep rooms that have water-damaged records well ventilated.**
- **Bring down temperature and humidity to help the water evaporate.**
- **If damage is sewer or hazardous waste leakage onto records, call Environmental Health and Safety (620-2019), as the area will need to be cleaned by Biohazard specialists.**
- **If microfilm or electronic media (tapes, disks, etc.) have gotten wet, keep them wet, do not let them dry.**

Salvage Priorities

Keep a list of items that should be salvaged first following a disaster for each department, area and/or office. Keep such considerations in mind when setting priorities.

- Is the item critical for ongoing operations of the institution?
- Can the item be replaced
- Would the cost of replacement be more or less than the cost of restoring the object? (Replacement cost figures should include ordering, cataloging, shipping, etc. in addition to the purchase price.)
- Is the item available in another format, or in secondary site?
- Does the item have a high or low priority?
- Does the item require immediate attention because of its composition (coated paper, vellum, water-soluble inks)?

Other Emergency Issues

Photographs of interior and exterior exist: (yes no) off-site? (yes no)

Is there an off-site record storage site? Is Data backup off-site?

Frequency of update: _____

Location/Contact: _____

Location/Contact: _____

Note: Records Management has Records Recovery text for use in the early stages of a disaster but recommends the services of professionals in records recovery.

Vital Records Checklist

Record Title:_____
Description of Function: _____
_____
Location: _____
Retention:_____
Format: Paper Tape Disk Photo

Answer the following questions for each record series evaluated:

1 What would not be processed if these records were destroyed?

2 Can the work be carried forward without the record?

3 What would the consequences to the University be?

4 How much of an impact would losing the records have on students and staff?

5 What would reconstruction costs be? (Time and money)

6 How quickly would the information need to be reproduced?
Why?

7 Can the records be replaced from another sources(s)? Where?

For Vital Records Only:

Protection Method:_____ Completed by:_____Location of other copies:_____Date: _____

DISASTER MANAGEMENT -- RECORDS

In the event of a disaster that totally disrupts operations, information for assistance and advice is readily available from those listed below. This list is not intended as recommended contractors listing but as quick resource

Staff members to be contacted in event of disaster:

Position	Name	Office	Cell	Home
CMT Chair and VP, Admin. & Finance	Shari Shuman	904-620-4727	904-338-6075	904-429-7831
Physical Facilities, Director	John Hale	904-620-1713	904-571-1071	904-724-5345
Physical Facilities, Assoc. Director	Wallace Harris	904-620-1310	904-704-9127	904-683-7589
Assoc. VP, Admin. & Fin.	Scott Bennett	904-620-2060	904-307-9939	904-821-9087
University Police Chief	Frank Mackesy	904-620-2396	904-591-6745	904-886-4935
CIO and Assoc. VP, Admin & Finance	TBD	904-xxx-xxxx	904-xxx-xxxx	904-xxx-xxxx

See University Crisis Management

Services Needed in an Emergency

Service Company and/or Contact Name Fire Department Duval County Fire Department Medical/Ambulance Medical

Emergency Dispatch

Hazardous Waste Disposal

Florida Environmental Compliance Corp. 8640 Phillips Hwy Jacksonville, Fl. 32 904-731-8959

Burns Services Inc. 400 9th Avenue, South Safety Harbor, Fl 34695 Laidlaw Environmental Services 1875 Forge Street Tucker, Ga. 30084 Records Management

Drying & Dehumidification

Air Quality Specialists318 Tarpon Drive Bay St. Louis, Ms 39520 228-467-8164 877-4DRY-AIR

Disaster Services Inc. 3030 Amwiler Road, Suite 1 Atlanta, Ga. 30360 770-446-5300
www.DISASTERSERVICES.com

Fire & Water Damage Restoration

Masters Disaster Restoration Services Inc. 1425 Old Ellis Road Atlanta, Ga. 30076 770-751-6151 Fax: 770-751-6150
www.disaster_restoration.com

NCRI – National Catastrophe Restoration, Inc. 3526 Comotara Wichita, Ks. 67226 316-636-5700 800-598-6274
www.ncricat.com

Smoke & Odor Counteracting Services

NCRI-National Catastrophe Restoration, Inc. 3526 ComotaraWichita, Ks. 67226 316-636-5700 800-598-6274 Records Management

Water Damage Restoration

NCRI-National Catastrophe Restoration Inc. 3526 ComotaraWichita, Ks. 67226 316-636-5700 800-598-6274
www.ncricat.com

Recover Water-Damaged Books & Documents

Burns Services Inc. 400 9 Avenue, South Safety Harbor, Fl 34695 727-726-1357
800-446-1620

Moisture Removal System Corp. 1471 Dale Court Austell, Ga. 30001 770-948-4700

National Restoration Contractors, Inc. 6065 NW 167 Street, Suite B1 Hialeah, Fl. 33015-4315 954-923-3090

TEC International 3274-Medlock Bridge Norcross, Ga. 30092 770-446-5400 800-526-1095

Documents Reprocessors 5611 Water Street Middlesex, N.Y. 14507 716-554-4500 Fax: 716-554-4114
www.documentreprocessors.com
Moisture Control Services 6900 Peachtree Industrial Blvd. Norcross, Ga. 30071-1028
770-242-0935

Microfilming & Record Copying

Anacomp7121 Grand National Dr.Orlando, Fl. 32819 813-885-3150
www.ANACOMP.com

Input Services Inc.1090 Northchase ParkwayMarietta, Ga. 30067-6400 770-952-8094

Offsite Tape, Film, Optical & Hard Copy Storage

Data Savers600 North Ellis Road Jacksonville, Fl. 32254 904-786-5749 Fax: 904-786-1294
www.datasaversfl.com

Iron Mountain5560 Shawland Road Jacksonville, Fl. 32254 904-783-260 Fax: 904-378-3076
www.ironmountain.com

Infoguard Inc. 6595 Pritchard Road Jacksonville, Fl 32219 904-783-7094 Fax: 904-783-7097
www.infoguardinc.com

Refrigeration and Freezing

Industrial Cold Storage 2625 W. 5 Street, PO. Box 41064 Jacksonville, Fl. 32203 904-786-8038

Ocala Cold Storage421 NE 14 Street Ocala, Fl. 34470 352-622-3272

Data Processing Site Specialists: Cleaning

Technical Restoration Services Inc. 5620 NW 12 Ave., Suite 103 Ft. Lauderdale, Fl. 33309
800-423-3182 GTE Data Services 1 East Telecom Parkway Temple Terrace, Fl. 33637
813-978-5163
www.GTE.com

Southern Micrographics 2861 Bankers Industrial #D Atlanta, Ga. 30360 770-729-8594

Filing Source, Inc./TAB 7529 Salisbury Road Jacksonville, Fl. 32256 904-398-3600
www.filingsource.com

Anacomp, Inc. 3728 Phillips Highway Jacksonville, Fl. 32208 904-936-9818
www.ANACOMP.com
Jaxport Refrigerated Services, Inc. 2701 Talleyrand Ave., PO Box 2639 Jacksonville, Fl. 32206 904-358-2206

Burris Refrigerated Logistics 2421 Dennis Street Jacksonville, Fl. 32204 904-353-4119

In-house Emergency Equipment

Vital Records

Administration Records for Grants/Contracts
Accounts Payable/Receivable
Consent Forms – Adult and Minor
Payrolls
Insurance policy information
Patents and Trademarks
Transcripts
Bid Documents
Capital Assets
Budget Records
Human Resource Records
Master Plan
Application for Internal Research Support--Awarded
Purchasing Leases and Contracts
Endowment Fund Records
General Ledgers
Committee Minutes
Research Data
Blueprints of Facilities
Police Records
Organization Charts and Listings
Deeds for University owned property
Student Records

Essential Records

Accreditation Documentation
Billing Source Documents
Grade Appeals
Annual/Monthly/Quarterly Reports
Current Calendars, Appointment Books, & Daily Schedules
Grievance Files

Useful Records

Bank Records
Equipment Maintenance/Service Reports
Subject files
Correspondence
Registrar's Statistical Reports – Copies

Natural Disasters	**Technical Disasters**	**Human Disaster**
Flooding	Power failure	Data entry
Fire	HVAC failure	Improper handling of sensitive data
Wind damage	Failure of CPU	Unauthorized access
Ice storm	Software failure	Destruction of data
Epidemic	Electromagnetic Interference	Robbery/theft/burglary
Vermin/insects	Explosion	Bomb threats
Hurricane	Telecommunications failure	Demonstrations/picketing
Lightning Strike	Gas Leaks	Civil disorder
Sink Hole		Chemical spill
		Vandalism
		Sabotage
		Hazardous material

Keys	Physical Plant – Bldg 6 – Richard McAuslin	2669 904-743-6532
Custodial	Physical Plant – Bldg 6 -	2933
Portable Pump	Physical Plant – Bldg 5 - Matthew Taylor	2490 904-230-8805
Extension Cords (50' grounded)	Physical Plant – Bldg 6 Rm 1237	2934
Flashlights	Physical Plant – Bldg 6 Rm 1237	2934
Wet-Vacuum	Physical Plant – Bldg 6	2933
Portable Folding Table	Student Affairs – Bldg 2	2600
Gloves	Physical Plant – Bldg 6 Rm 1237	2934
First Aid	Student Health Center – Bldg 14	2900
Heavy Plastic Sheeting	Physical Plant – Bldg 6 Rm 1237	2934
Paper Towels	Physical Plant – Bldg 6 Rm 1237	2934
Plastic Garbage	Physical Plant – Bldg 6 Rm 1237	2934

Additional Sources of Emergency Equipment and Supplies

Portable Dehumidifiers	Granger Ind. Supply	8450 Phillips Hwy.	636-8896
Portable Fans	Granger Ind. Supply	8450 Phillips Hwy.	636-8896
Hard Hats	Granger Ind. Supply	8450 Phillips Hwy.	636-8896
Rubber Boots	Granger Ind. Supply	8450 Phillips Hwy.	636-8896
Rubber Gloves	Granger Ind. Supply	8450 Phillips Hwy.	636-8896
Rubber/Plastic Aprons	Granger Ind. Supply	8450 Phillips Hwy.	636-8896
Portable Pumps	Acme Dynamics, Inc.	10845 Phillips Hwy.	262-2405

Refrigerator Trailers T & T Trailer Rental	625 N. Ellis Road	783-1130
Portable Lighting Ring Power Systems	8040 Phillips Hwy.	737-7730
Plastic Buckets Granger Ind. Supply	8450 Phillips Hwy.	636-8896

Appendix A

CHAPTER 1B-24 PUBLIC RECORDS SCHEDULING AND DISPOSITIONING

1B-24.001 General. 1B-24.002 Definitions. (Repealed) 1B-24.003 Records Retention Scheduling and Disposition. 1B-24-004 Developing Requests for Records Retention Schedules. (Repealed) 1B-24.005 Submitting Proposed Records Retention Schedules. (Repealed) 1B-24.006 Division Criteria for Processing Proposed Records Retention Schedules. (Repealed) 1B-24.007 Division Action. (Repealed) 1B-24.008 Revising Records Retention Schedules. (Repealed) 1B-24.009 General Records Schedules. (Repealed) 1B-24.010 Records Disposition. (Repealed) 1B-24.011 Division Criteria for Approval of Records Disposition Requests. (Repealed) 1B-24.012 Disposition Certificate. (Repealed) 1B-24.013 Penalty for Violation. (Repealed)

1B-24.001 General

(1) This chapter establishes standards and procedures for the scheduling and dispositioning of records to promote economical and efficient management of records and to ensure that records of archival value under an agency's control are so designated and ultimately transferred to the Florida State Archives.
(2) Each agency in the State of Florida is responsible for complying with provisions of this chapter.
(3) For the purpose of this chapter:

a) "Agency" means any state, county, or municipal officer, department, district, division, board, bureau, commission or other separate unit of government created or established by law.
b) "Custodian" means the elected or appointed state, county, district, or municipal officer charged with the responsibility of maintaining the office having public records, or his or her designee.
c) "Database Management System" means a set of software programs that controls the organization, storage, and retrieval of data (fields, records and files) in a database. The system also controls the security and integrity of the database.
d) "Division" means the Division of Library and Information Services of the Department of State.
e) "Florida State Archives" means the program maintained by the Division for preservation of those public records and other papers that have been determined by the Division to have sufficient historical or other value to warrant their continued preservation by the State and which have been accepted by the Division for deposit in its custody.
f) "General Records Schedules" means retention requirements issued by the Division to establish disposition standards for public records common to specified agencies within the State of Florida which state the minimum time such records are to be kept.
g) "Electronic Records" means any information that is recorded in machine-readable form. h) "Public Records" are those as defined in Section 119.011, Florida Statutes. i) "Record (Master Copy)" means public records specifically designated by the custodian as the official record.
j) "Duplicate (or Convenience) Records" means reproductions of record (master) copies, prepared simultaneously or separately, which are designated as not being the official copy.
k) "Record Series" means a group of related documents arranged under a single filing arrangement or kept together as a unit because they consist of the same form, related to the same subject, result from the same activity, or have certain common characteristics.
l) "Records Retention Schedule" means a standard approved by the Division for the agency's orderly retention, transfer, or disposition of public records taking into consideration their legal, fiscal, historical, and administrative values.
m) "Records Management Liaison Officer" means an individual designated by the agency that serves as a contact person to the Division and is assigned responsibilities by the Custodian.
n) "Intermediate Records" (Processing Files) are temporary records used to create, correct, reorganize, update, or derive output from master data files. Intermediate records are precursors of public records, and are not, in themselves, public records that must be retained. Intermediate records only exist provided a final product is subsequently generated which perpetuates, communicates, or formalizes knowledge of some type. In the absence of such a final product, processing files constitute final evidence of the knowledge to be recorded and shall not be construed as intermediate files for the purposes of this chapter.
o) "Supporting Documents" means public records assembled or created to be used in the preparation of other records which are needed to trace actions, steps, and decisions covered in the final or master record.
p) "Drafts" are materials, which constitute precursors of governmental "records" and are not, in themselves, intended as final evidence of the knowledge to be recorded. Information in a form which is not intended to perpetuate, communicate, or formalize knowledge of some type and which is fully represented in the final product is a "draft" and not a "public record."

Specific Authority 257.14, 257.36(6) FS. Law Implemented 257.36 FS. History-New 1-8-80, Formerly 1A-24.01, 1A24.001, Repromulgated 3-23-93, Amended 2-20-01.

1B-24.003 Records Retention Scheduling and Dispositioning.

1) Each agency shall submit to the Division a request for records retention on Department of State Form LS5E 105R Eff. 1-01, "Records Retention Schedule" which is hereby incorporated by reference and made part of this rule, for all records series. A copy of Form LS5E 105R Eff.1-01, effective, January 2001, may be obtained from the Bureau of Archives and Records Management, Department of State, Mail Station 9A, The Capitol, Tallahassee, Florida 32399-0250. This schedule shall be developed to reflect the legal, fiscal, historical and administrative requirements of the agency for each record series. The schedule shall designate whether the series constitutes a record (master) copy or duplicate. Form LS5E 105R Eff. 1-01 is to be signed by the custodian of the records, or his or her designee, and submitted to the Division for determination of official retention requirements.
2) Retention and scheduling of intermediate files are not feasible due to their transitory nature, and do not require submission of Form LS5E 105R Eff. 1-01 "Records Retention Schedule".
3) Each Records Retention Schedule is analyzed by the Division in the context of an agency's statutory functions and authorities, Florida Statutes, administrative rules, operating procedures, applicable federal regulations and other such sources shall be researched to assist in the determination of a record's value.
4) In addition, the Records Retention Schedule is reviewed to determine whether the records merit further retention by the State in the Florida State Archives. This determination is based upon whether the records have significant legal, fiscal administrative or historical information value to merit such further retention. The main objectives of this determination are to preserve those records pertaining to the operation of government and to protect the rights and interest of the citizens of the state.
5) In the event that records are of archival value, an indication is made on the Records Retention Schedule that such historical records are to be transferred to the Florida State Archives as part of the retention requirements.
6) Local government records having archival value may be loaned to local historical records repositories for preservation provided they are maintained under the provisions of Chapter 119, Florida Statutes.
7) The Division, with information submitted on Form LS5E 105R Eff. 1—1, "Records Retention Schedule" and its own research into the legal, fiscal, historical and administrative value of the record series, shall create an official "Records Retention Schedule. Once approved by the Division, the Records Retention Schedule becomes the official retention for the record series of the submitting agency.
8) After an agency has established an approved Records Retention Schedule in accordance with the foregoing procedures, it may become apparent that the schedule needs to be revised. When changes are necessary, the specific records series of the approved schedule shall be resubmitted by the agency, with an appropriate explanation for the revision. The approved Records Retention Schedule shall receive the next consecutive number.
9) General Records Schedules are originated by the Division and are used by agencies designated by the Division. Utilization of General Records Schedules eliminates the need to comply with provisions of Rule 1B-24.003(1), F.A.C. of this chapter.
10) Prior to records disposition, an agency must ensure that retention requirements have been satisfied. The minimum requirements for each records disposition is the identification and documentation of the following:

- schedule number;
- item number;
- record series title;
- the inclusive dates;

and the volume in cubic feet. A public record may be destroyed or otherwise disposed of only in accordance with retention schedules established by the Division. Photographic reproductions or reproductions or reproductions through electronic recordkeeping systems may substitute for the original or paper copy, per Section 92.29, F.S. Minimum standards for image reproduction shall be in accordance with 1B-26.0021 and 1B-24.003, Florida Administrative Code.

11) Each agency shall submit to the Division, once a year, a signed statement attesting to the agency's compliance with records disposition laws, rules, and procedures.
12) Any record series identified, by either a General Records Schedule or approved Records Retention Schedule, indication archival value cannot be destroyed without the approval of the Florida State Archives.
13) The Division shall compile an annual summary of agency records scheduling and disposition activities to inform the Governor and the Legislature on statewide records management practices and program compliance.

Specific Authority 257.36 FS Law Implemented 257.36 FS. History-New 2-20-01.

Appendix B

1B-26.003 Electronic Recordkeeping.
(1) PURPOSE. These rules provide standards for record (master) copies of public records which reside in electronic recordkeeping systems. Record keeping requirements must be incorporated in the design and implementation of new systems and enhancements to existing systems. Public records are those as defined by Section 119.011(1), Florida Statutes.
(2) AUTHORITY. The authority for the establishment of these rules is Section 257.36(1) and (7)(c), Florida Statutes.
(3) SCOPE.
(a) 1. These rules are applicable to all agencies as defined by Section 119.011(2), Florida Statutes.

1. These rules establish the minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposition of record (master) copies, regardless of the media.
2. Electronic records include numeric, graphic, sound, video, and textual information which are in or transmitted in analog or digital form.
3. These rules apply to all electronic recordkeeping systems, including, but not limited to, microcomputers, minicomputers, mainframe computers, or image recording systems (regardless of storage media) in network or stand-alone configuration.

(b) Before existing records are committed to an electronic recordkeeping system, the agency shall conduct a cost benefit analysis to insure that the project or system contemplated is cost effective.
(c) Any electronic recordkeeping system not meeting the provisions of these rules may be utilized for long-term or permanent records provided the record (master) copy is maintained or microfilmed in accordance with the provisions of Rule IB-26.0021, F.A.C. prior to disposition.
(4) INTENT. Electronic recordkeeping systems in use at the effective date of this rule that are not in compliance with requirements of this rule, may be used until the systems are replaced or upgraded. New and upgraded electronic recordkeeping systems created after the effective date of this rule shall comply with the requirements contained herein. The Department is aware that it may not be possible to implement this rule in its entirety immediately upon its enactment, and it is not the intent by this rule to disrupt existing recordkeeping practices provided that agencies make no further disposition of public records without approval of the Division of Library and Information Services of the Department of State.
(5) DEFINITIONS. For the purpose of these rules:
(a) "Database" means an organized collection of automated information.
(b) "Database management system" means a set of software programs that controls the organization, storage and retrieval of data (fields, records and files) in a database. It also controls the security and integrity of the database.
(c) "Data file" means related numeric, textual, sound, video, or graphic information that is organized in a prescribed form and format.
(d) "Electronic record" means any information that is recorded in machine-readable form.
(e) "Electronic recordkeeping system" means an automated information system for the organized collection, processing.
(f) "System design" means the design of the nature and content of input, files, procedures, and output and their interrelationships.
(g) "Permanent or Long-term records" means any public records which have an established retention period of more than 10 years. See Section 119.011 (1), F. S. for the definition of a public record.
(h) “Record (master) copy” means public records specifically designated by the custodian as the official record.
(i)“Geographic information system” means a computer system for capturing, storing checking, integrating, manipulating, analyzing and displaying data related to positions on the Earth’s surface.
(j) “Open format” means a data format that is defined in complete detail and that allows transformation of data to other formats without loss of information. An open format may be either standards-based or proprietary.
(6) AGENCY DUTIES AND RESPONSILITIES. The head of each agency shall:
(a) Develop and implement a program for the management of electronic records.
(b) Ensure that all records are included with records retention schedules, either by being included within an applicable General Records Schedule, or by developing and obtaining approval for a specific records retention schedule. Each record series shall be considered on an individual basis by the Division of Library and Information Services in establishing this retention period. See subsection 1B-24.001(3), F.A.C., for the definition of a record series.
(c) Integrate the management of electronic records with other records and information resources management programs of the agency.
(d) Incorporate electronic records management objectives, responsibilities, and authorities in pertinent agency directives, or rules, as applicable.
(e) Establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving, recommending, adopting, or implementing new electronic recordkeeping systems or enhancements to existing systems.
(f) Provide training for users of electronic records systems in the operation, care, and handling of the equipment, software, and media used in the system.
(f) Develop and maintain documentation about electronic recordkeeping systems in the operation, care, and handling of the equipment, software, and media used in the system.
(g) Ensure that electronic recordkeeping systems meet state requirements for public access to records.

1. STANDARD. Each agency that maintains public records in an electronic recording system shall provide, to any person making a request pursuant to Chapter 119, F.S., a copy of any data in such records, which is not specifically exempt. Said copy shall be on paper, disk, tape, optical disk, or any other electronic storage device or media requested by the person, if the agency currently maintains the record in that form, or as otherwise required by Chapter 119, F.S. Except as otherwise provided by state statute, the cost for providing a copy such data shall be in accordance with provisions of Sections 119.07(1)(a) and (b), F.S.
2. STANDARD. Except as otherwise provided by law, no agency shall enter into a contract with, or otherwise obligate itself to, any person or entity if such contract or obligation impairs the right of the public under state law to inspect or copy the agency's nonexempt public records existing on-line in, or stored on a device or media used in connection with, a computer system or optical imaging system owned, leased or otherwise used by an agency in the course of its governmental functions.
3. STANDARD. Each agency shall insure that current and proposed electronic recordkeeping system adequately provide for the rights of the public to access public records under Chapter 119, F.S.
4. STANDARD. In addition to ensuring that electronic record keeping systems meet requirements for public access to public records, agencies shall ensure that procedures and controls maintain confidentiality for information that is exempt from public disclosure.

(h) Develop and maintain documentation about electronic recordkeeping systems used by the agency to specify technical characteristics necessary for reading or processing the records. Documentation for electronic records systems shall meet the following standards:

1. STANDARD. Each agency shall identify all inputs and outputs of the system; define the organization and contents of the files and records; define policies on access and use; define the purpose and function of the system; define update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and ensure the timely, authorized disposition of the records in accordance with Chapter 1B-24, F.A.C.
2. STANDARD. Each agency shall specify the location and media in which electronic records are maintained to meet retention requirements, establish and document security controls for the protection of the records, and maintain inventories of electronic recordkeeping systems to facilitate disposition.

(7) DOCUMENTATION STANDARDS.
(a) STANDARD. Agencies shall maintain adequate and up-to-date technical documentation for each electronic recordkeeping system. Documentation for electronic records systems shall be maintained in printed form, and should also be maintained in computer-readable form to facilitate access to the records. The minimum documentation required is:

1. a narrative description of the system;
2. The physical and technical characteristics of the records, including a record layout or markup language that describes each field including its name, size, starting or relative position, and description of the form of the data (such as alphabetic, decimal, or numeric), or a data dictionary or the equivalent information associated with a database management system including a description of the relationship between data elements in data bases;
3. For information coming from geographic information systems, the physical and technical characteristics of the records must be described including a data dictionary, a quality and accuracy report and a description of the graphic data structure, such as recommended by the federal Spatial Data Transfer Standards; and
4. Any other technical information needed to read or process the records.

(8) CREATION AND USE OF ELECTRONIC RECORDS AS RECORD (MASTER) COPIES. Electronic recordkeeping systems that maintain record (master) copies of public records on electronic media shall meet the following minimum requirements:
(a) l. Provide a method for all authorized users of the system to retrieve desired records;

1. Provide an appropriate level of security to ensure the integrity of the records, in accordance with the requirements of Chapter 282, F.S. Security controls should include, at a minimum, physical and logical access controls, backup and recovery procedures, and training for custodians and users. Automated methods for integrity checking should be incorporated in all systems that generate and use official file copies of records. Hashing algorithms and digital signatures should be considered for all official file copies of electronic records. The use of automated integrity controls, such as hashing algorithms and digital signatures, can reduce the need for other security controls. Hashing algorithms used protect the integrity of official file copies of records should meet requirements of US Federal Information Processing Standard Publication 180-1 (FIPSPUB 180-1) (April 17, 1995) entitled "Secure Hash Standard," which is hereby incorporated by reference, and made a part of this rule. This publication is available from the National Technical Information Service (NTIS), 5285 Port Royal Road, U.S. Department of Commerce, Springfield, VA 22161, and at the Internet Uniform Resource Locator: Records Management 180-1.htm. Agencies should also consider using only validated implementations of hashing algorithms in cases where the data being protected are of great intrinsic value or where the content and authenticity of the records are likely to be at issue in litigation.
2. Identify the open format or standard interchange format when necessary to permit the exchange of records on electronic media between agency electronic recordkeeping systems using different software/operating systems and the conversion or migration of records on electronic media from one system to another. For text records in the absence of other conversion capabilities, the word processing or text creation system should be able to import and export files in the ASCII format as prescribed by Federal Information Processing Standard Publication (FIPS PUB) Number 1-2; entitled Coded Character Sets

– 7 Bit American National Standard Code for Information Exchange (7—Bit ASCII) (1986, R2002), which is hereby incorporated by reference, and made a part of this rule.

This publication is available from the National Technical Information Service (NTIS), 5285 Port Royal Road, U.S. Department of Commerce, Springfield, VA 22161; and
4. Provide for the disposition of the records including, when appropriate, transfer to the Florida State Archives.
(b) STANDARD. Before a record (master) copy is created on electronic recordkeeping systems, the record shall be uniquely identified to enable authorized personnel to retrieve, protect, and carry out the disposition of records in the system. Agencies shall ensure that records maintained in such systems can be correlated with any existing related records on paper, microfilm, or other media.
(9) LEGAL AUTHENTICATION. Agencies shall implement the following procedures to enhance the legal admissibility of electronic records:
(a) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.
(b) Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure systems protection against such problems as power interruptions.
(c) Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage media, and the official retention requirements as approved by the Division of Library and Information Services.
(d) State agencies shall, and other agencies are encouraged to, establish and maintain integrity controls for record (master) copies of electronic records in accordance with the requirements of Chapter 282, F.S.
(10)SELECTION OF ELECTRONIC RECORDS STORAGE MEDIA. For storing record (master) copies of public records throughout their life cycle, agencies shall select appropriate media and systems that meet the following requirements:
(a) Permit easy and accurate retrieval in a timely fashion;
(b) Retain the records in a usable format until their authorized disposition and, when appropriate, meet the requirements necessary for transfer to the Florida State Archives.
(c) Obtain recording media only from vendors whose guarantee of 10 years or more of readability is based upon documented accelerated aging tests that are linked to specific locations on the media.
(d) STANDARD. A scanning density with a minimum of 300 dots per inch will be required for recording electronic records.
(e) STANDARD. Record (master) copies of digital images must be stored in accordance with the TIFF 6.0 specification (June 3, 1992), which is hereby incorporated by reference and made a part of this rule. This specification is available from the Aldus Corporation, 411 First Avenue South, Seattle, WA 98104-2871. If use of a proprietary image format is unavoidable, the agency must provide a gateway to lossless conversion to the TIFF 6.0 specification.
(f) STANDARD. Any optical media application system will support either Group 3 or Group 4 compression techniques as specified in the Consultative Committee on International Telegraphy and Telephones "Blue Book, Volume 7.3", which is hereby incorporated by reference and made a part of this rule. This volume is available from the International Telecommunications Union, Consultative Committee, Place des Nations, CH-1211, Geneva 20, and Switzerland. If use of a proprietary compression technique is unavoidable, the vendor should be required to provide a gateway to either Group 3 or Group 4 compression techniques.
(g) The following factors are to be considered before selecting a storage media or converting from one media toanother:

1 The authorized retention of the records as determined during the scheduling process;
2 The maintenance necessary to retain the records;
3 The cost of storing and retrieving the records;
4 The access time to retrieve stored records;
5 The portability of the medium (that is, selecting a medium that can be read by equipment offered by multiple manufactures); and
6 The ability to transfer the information from one medium to another such as from optical disk to magnetic tape.

(11) MAINTENANCE OF ELECTRONIC RECORDS.
(a) STANDARD. Agencies shall maintain all long-term and permanent backup/security electronic recording media in a storage facility, either on-site or off-site, with constant temperature (below 68 degrees Fahrenheit) and relative humidity (20 to 30 percent) controls. Storage and handling of long-term and permanent records on magnetic tape shall conform to the standards contained in Standard AES22-1997 "AES recommended practice for audio preservation and restoration – Storage and handling – Storage of polyester-base magnetic tape," (1997) which is hereby incorporated by reference and made a part of this rule. This publication is available from the Audio Engineering Society, Incorporated, to East 42nd Street, Room 2520, New York, New York, 101652520.
(b) STANDARD. Agencies shall annually read a statistical sample of all electronic media containing long-term or permanent records to identify any loss of information and to discover and correct the cause of data loss.
(c) STANDARD. Agencies shall test all long-term or permanent electronic records at least every 10 years and verify that the media are free of permanent errors.
(d) STANDARD. Agencies shall only rewind tapes immediately before use to restore proper tension. When tapes with extreme cases of degradation discovered, they should be rewound to avoid more permanent damage. Tapes shall be played continuously from end to end to ensure even packing. Tapes shall be stored so that the tape is all on one reel or hub.
(e) STANDARD. Agencies shall prohibit smoking, eating, and drinking in areas where electronic records are created, stored, used, or tested.
(f) STANDARD. External labels (or the equivalent automated management system) for electronic recording media used to store long-term or permanent records shall provide unique identification for each storage media, including:

1 The name of the organizational unit responsible for the data;
2 System title, including the version number of the application;
3 Special security requirements or restrictions on access, if any; and,
4 Software in use at the time of creation.

(g) STANDARD. For each electronic records series, agencies shall maintain human readable information specifying the metadata associated with series, and technical documentation specifying recording methods, formats, languages, dependencies, and schema sufficient to ensure continued access to, and intellectual control over, the series. Additionally, the following information shall be maintained for each media used store long-term or permanent electronic records:
1. File title;
2. Dates of creation;
3. Dates of coverage;

5. Character code/software dependency.
(h) STANDARD. Electronic records shall not be stored closer than 2 meters from sources of magnetic fields, including generators, elevators, transformers, loudspeakers, microphones, headphones, magnetic cabinet latches and magnetized tools.
(i) STANDARD. Electronic records on magnetic tape or disk shall not be stored in metal containers unless the metal is non-magnetic. Storage containers shall be resistant to impact, dust intrusion and moisture. Compact disks shall be stored in hard cases, and not in cardboard, paper or flimsy sleeves.
(j) STANDARD. Agencies shall ensure that record (master) copies of electronic records are maintained by personnel properly trained in the use and handling of the records and associated equipment.
(k) STANDARD. Agencies shall not use floppy disks, audio cassettes, or VHS-format video cassettes for the storage of record (master) copies of long-term or permanent records. Long-term and permanent records on magnetic tape shall be stored on polyesterbased media. Agencies shall use only previously unrecorded videotape for original record (master) copies of long-term or permanent video recordings. For long-term or permanent tapes at three and three-quarters or seven and one half inches per second, full track, using professional unrecorded polyester splice-free tape stock. For long term or permanent digital recordings of record (master) copies, agencies may use open reel one-half inch tape reels recorded at 1600 or more bits-per-inch; 3480,3490, or 3590-type tape cartridges; or compact disk read-only-memory (CD-ROM) media.
(l) Agencies shall establish and adopt procedures for external labeling of the contents of diskettes, disks, tapes, or optical disks so that all authorized users can identify and retrieve the stored information.
(m) Agencies shall convert storage media to provide compatibility with the agency's current hardware and software to ensure that information is not lost due to changing technology or deterioration of storage media. Before conversion of information to different media, agencies must determine that authorized disposition of the electronic records can be implemented after conversion. Long-term or permanent electronic records stored on magnetic tape shall be transferred to new media as needed to prevent loss of information due to changing technology or deterioration of storage media.

(n) Agencies shall back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of long-term or permanent records shall be maintained in storage areas located in buildings separate from the location of the records that have been copied.
(12) RETENTION OF ELECTRONIC RECORDS. Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed. These retention procedures will include provisions for:
(a) STANDARD. Scheduling the retention and disposition of all electronic records, as well as related access documentation and indexes, in accordance with the provisions of Chapter lB-24, F.A.C.
(b) STANDARD. Transferring a copy of the electronic records and any related documentation and indexes to the Florida State Archives at the time specified in the records retention schedule, if applicable. Transfer may take place at an earlier date if convenient for both the agency and the Archives.
(c) STANDARD. Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of the electronic records throughout their authorized life cycle.
(13) DESTRUCTION OF ELECTRONIC RECORDS. Electronic records may be destroyed only in accordance with the provision of Chapter lB-24, F.A.C. At a minimum each agency should ensure that:
(a) Electronic records scheduled for destruction must be disposed of in a manner that ensures protection of any sensitive, proprietary, or security information, and;
(b) Recording media previously used for electronic records containing sensitive, proprietary, or security information are not reused if the previously recorded information can be compromised in any way by reuse.

Specific Authority 257.14,257.36(7)FS. Law Implemented 257.36(1)(a) FS. History-New 8-16-92 Amended 5-13-03.

Appendix C

Florida Attorney General Advisory Legal Opinion Number: AGO 85-87 Date: October 25, 1985

Subject: Machine readable files, public records

The Honorable George Firestone Secretary of State The Capitol Tallahassee, Florida 32301

Dear Secretary Firestone:

This is in response to your request for an opinion on the following questions:

1 Are machine-readable intermediate files "Public Records" within the meaning of Chs. 119 and 267, Florida Statutes?
2 If machine-readable intermediate files are indeed "public records," who is the legal custodian as defined by s. 119.021, Florida Statutes--the owner agency of the raw data, or the data center which created the intermediate documents?

As qualified herein, your first question is answered in the negative, such that no response is required to your second question. With respect to the nature of "intermediate files" in the computer data processing context, your inquiry informs me as follows:

> As part of the task of manipulating data from input file to output file, any number of "intermediate" files may be generated. These intermediate files have been described to division staff by personnel from AMIC (Administrative Management Information Center) as "tools" used to create the final intended product that represents final evidence of the knowledge to be recorded. Often, the owner agency (the custodian) of the raw data and the final product is unaware of the existence of these intermediate documents and is only concerned with the final output file(s). Intermediate files may occasionally exist for only a few seconds as magnetic code on the hard disk of a large computer installation or on the floppy disk of a personal computer or word processor and their contents are rarely if ever reviewed by any person. By their nature, intermediate files do not lend themselves to the scheduling and dispositioning process as outlined by Chapter 1A-24 Florida Administrative Code. Additionally, custodianship and access problems exist due to the transitory nature of intermediate files and the lack of knowledge by the owner agency of the very existence of these files.
>
> Your staff has further advised this office that these intermediate files are distinguishable from computer programs, which are also "tools" but which are used to retrieve information stored in a computer in a specified format and at high speed. To illustrate, the application of a program to the data supplied to or stored in the computer results in the creation of machine-readable intermediate files that enable the computer to assemble the data in the requested manner in order to produce an output document of some type (e.g., a printout or a disk or tape). Additionally, your inquiry notes that it is your view that [input documents [and output documents] are clearly public records ... and lend themselves to the scheduling and dispositioning process as outlined in Chapter 1A-24 Florida Administrative Code." See also, s. 267.051(1), F.S., imposing certain records management duties and responsibilities upon the Division of Archives, History and Records Management of the Department of State.

Sections 119.011(1) and 267.021(2), F.S., provide substantially identical definitions of the term "Public Records." For purposes of Ch. 119, F.S., s. 119.011(1), supplies the following definition:

> "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

There can be no doubt that information stored on a computer is as much a public record as a written page in a book or a tabulation in a file stored in a filing cabinet. Seigle v. Barry, 422 So.2d 63, 65 (4 D.C.A.Fla., 1982). See, AGO 85-3 (computer tapes are public records). However, although the court in the Seigle case also suggested that "all of the information in the computer ... should be available for examination and copying in keeping with the public policy underlying the [Public Records Act]," I am of the view that your inquiry is controlled by the judicial construction of s. 119.011(1) in Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc., 379 So.2d 633 (Fla.1980).

To give content to the public records law which is consistent with the most common understanding of the term "record," we hold that a public record, for purposes of section 119.011(1), is any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type. To be contrasted with "public records" are materials prepared as drafts or notes, which constitute mere precursors of governmental "records" and are not, in themselves, intended as final evidence of the knowledge to be recorded. Matters that obviously would not be public records are rough drafts, notes to be used in preparing some other documentary material, and tapes or notes taken by a secretary as dictation. Inter-office memoranda and intra-office memoranda communicating information from one public employee to another or merely prepared for filing, even though not a part of an agency's later, formal public product, would nonetheless constitute public records inasmuch as they supply the final evidence of knowledge obtained in connection with the transaction of official business. (e.s.) 379 So.2d at 640.

From the description of "machine-readable intermediate files" furnished with your inquiry, it would deem that such files are not intended to perpetuate or formalize knowledge of some type but rather constitute mere precursors of governmental records and are not, in themselves, intended as final evidence of the knowledge to be recorded. Moreover, to the extent that such machine-readable files may be intended to "communicate" knowledge, the facts as stated in your inquiry would indicate that such communication takes place completely within the data processing equipment and in such form as to render any "inspection or examination" pursuant to Ch. 119, F.S., unintelligible and, except perhaps to the computer itself, meaningless. Thus, such machine-readable intermediate files would appear to be analogous to notes used to prepare some other documentary material and, under the construction of s. 119.011(1), F.S., in Shevin v. Byron, Harless, supra, are not "public records" for purposes of Chs. 119 and 267, F.S.

Therefore, unless and until legislatively or judicially determined otherwise, it is my opinion that machine-readable intermediate files which are mere precursors of governmental records and are not, in themselves, intended as final evidence of the knowledge to be recorded but rather are utilized by data processing computer equipment to prepare further records which are intended to perpetuate, communicate, or formalize knowledge of some type are not "public records" within the meaning of Chs. 119 and 267, F.S.

Sincerely,

Jim Smith Attorney General

Prepared by:
Kent L. Weissinger
Assistant Attorney General

Appendix D

DEPARTMENT OF STATE ELECTRONIC MAIL OPINION

Department of State Memorandum

Office of the General Counsel

TO: Jim Berberich, Bureau of Archives & Records Management FROM: Donald L. Bell, General Counsel DATE: November 9, 1995 RE: 81-DS-L

Electronic Mail and Transitory Messages Ch.lB-24, F.A.C.; Ch.119, Fla. Stat. (1993); and 36 C.F.R.§§ 1220 et al.(1995)

This is in response to your recent inquiry regarding electronic mail (e-mail).

BACKGROUND

Many state agencies, including the Department of State (DOS), are now capable of sending and receiving e-mail. As the agency responsible for establishing record retention standards, DOS has received numerous inquiries from other agencies and from the public with regard to whether e-mail is subject to the retention requirements for public records and, if so, how e-mail should be processed for retention. You have asked me to address certain legal issues relating to this topic.

RETURN TO LIST OF TOPICS

ISSUES

1. **Are e-mail messages public records within the meaning of Chapter 119, Florida Statutes?**
2. **If e-mail messages are public records, are they subject to DOS's existing record retention requirements and standards?**
3. **If e-mail messages are public records, should DOS develop new rules for administration of e-mail systems?**

SHORT ANSWER

Some e-mail messages are public records within the meaning of Chapter 119, Florida Statutes; other messages are not. E-mail messages that are not public records need not be retained. E-mail messages that are public records should be retained in accordance with DOS rules. DOS's record retention standards are not based on the method by which a record is created. Rather, retention periods are established based on the legal, fiscal, administrative or historical value of the information contained in the records. Therefore, the application of DOS retention periods would not change simply because a record is transmitted electronically. For example, DOS schedules require the retention of certain memoranda and correspondence for specified time periods. Transmitting such records electronically would not alter the obligation to retain these records, nor would it alter their corresponding retention periods.

In most instances, the existing schedules for retention of public records adequately address issues that might arise relating to e-mail. However, in addition to retention periods, DOS has often established rules and offered advice to agencies regarding such matters as public access and retention and storage methods. Unless DOS dictates specific methods for retention, e-mail messages that are public records may be stored and retained by any means that assures safe maintenance and public accessibility throughout the appropriate retention period. This could mean storage on a magnetic disk or hard drive, or by printing the messages and filing them in a traditional filing system. We recommend that DOS refrain from creating additional rules to specify retention methods. The nature of e-mail and computer systems may vary greatly from one agency to the next, and agencies should be free to make their own decisions regarding the most suitable means of retention. However, given that there is some confusion on this subject, DOS should consider whether e-mail is of such a unique nature that agencies would benefit from additional guidance. Consistent with recent policy decisions that favor agency discretion over rule- making, if you determine that DOS should offer some additional guidance in these areas, we recommend that advisory information be made available through non-rule guidelines.

Finally, in reviewing recent legal developments relating to non-traditional communications such as e-mail, we note that courts and other authorities have begun to recognize the existence of "transitory" communications. Largely a by- product of the electronic age, transitory messages have some administrative value. These messages are created without any intention to perpetuate or formalize knowledge. They have only communicative value which is lost as soon as the communication is received. Despite the fact that they have only limited administrative value, transitory communications must be considered public records under Florida law and must be treated as such.

DOS has recognized that requiring permission to dispose of certain records with limited retention value would impose an unreasonable economic and administrative burden on persons or entities that are subject to the public records Electronic Mail Opinion law. Therefore, DOS has permitted disposition of records that have an "obsolete, superseded, or administrative value is lost" (OSA) retention schedule without further approval from DOS. DOS should establish a new record series that covers "transitory messages" with a retention value of OSA, just as it has one for record (Master) copies and duplicate records In Rule 1B-24.010(3), Florida Administrative Code.

RETURN TO LIST OF TOPICS

DISCUSSION

Official business and non-business e-mail:

In examining its own use of e-mail, the Supreme Court of Florida as established that “official business e-mail transmissions must be treated just like any other type of official communication," and that "official business communicated by e-mail transmissions is a matter of public record." In re: Amendments to Rule of Judicial Administration 2.051-- Public Access to Judicial Records, 651 So. 2d 1185 (Fla. 1995). However, the court has also recognized that e-mail messages may include transmissions that are not official business and which, consequently, are not public records." id. at 1187. Thus, the Supreme Court has already given us some guidance in this area. Non-business e-mail messages are not public records and need not be retained. id. All other e-mail messages are public records.

Public policy and e-mail public records:

In addressing retention requirements for public records transmitted by-mail, we must consider the underlying public policy considerations that cause us to require the retention of public records, the reasons for using e-mail, and the natural inclinations of the people who use e-mail systems. The underlying purpose for retaining public records is to assure" agency policies, functions, transactions, and decisions are properly documented." 36 C.F.R. Part 1220 et al. (Electronic E-Mail Systems) ("E-Mail Comments"), Federal Register On-line, Comment No.8 at 44637. While retention requirements must serve this basic function, failure to comply with record retention requirements may constitute a criminal violation. § 119.02, Fla. Stat. (1993). Thus, we must be certain that we do not impose unreasonable or unrealistic standards that might cause natural or unintentional behavior to be characterized as unlawful.

> In considering appropriate retention periods, DOS must also be cautious that it does not have" a chilling effect that would limit the use and usefulness of e-mail." E-Mail Comments, Comment No.4 at 44636. Many users of e-mail believe that the "informal nature of e-mail messages is the main attraction of the system." id. Many, if not most, e-mail messages are" casual and routine communications similar to telephone conversations." See General Letter No. 95-1, from Eunice G. DiBella, Connecticut Public Records Administrator, E-Mail Guidelines for Public Officials (June 1, 1995) (hereinafter "Connecticut E-Mail Policy"). The Supreme Court of Florida has noted that e-mail is often used as a modern "substitute for telephonic and printed communications, as well as a substitute for Electronic Mail Opinion direct oral communications." In re: Amendments to Rule of Judicial Administration 2.051,651 So. 2d at 1186.

Experience in our office indicates that many e-mail messages consist of one or two lines dashed off electronically because, at any given time, it may be the most expedient means of communicating a simple message: "your meeting is at 2:00, don't be late"; "remember to order a new copier cartridge this afternoon"; "please let me know when you will have the project finished." These communications are the electronic equivalent of communications that under different circumstances would take place verbally --either by telephone or directly. E-mail is used to substitute for a shout down the hallway when the distance is too great to shout without disturbing others or when a shout would be considered rude; for communicating with a colleague who may be temporarily preoccupied; or, for dashing off a quick thought to someone before the thought escapes our attention. In contrast to the traditional practice, which is to reduce important thoughts to writing, messages are often communicated by e-mail because they are of lesser importance. Information of greater importance is formalized into letters or memoranda.

As noted, e-mail users are attracted to this form of communication due to expediency and informality. E-Mail Comments, Comment No.4 at 44636. By unnecessarily imposing rules that are designed for more formal records, we would "inappropriately formalize the communications and, in this way, inhibit usage." id. We would also "place unreasonable burdens on staff, would reduce productivity, and would destroy rapid communication, the most important feature of e-mail." id.

"[E]-mail has a major role in the efficiency of communications." E-Mail Comments, Comment No.1 at 44635. We must exercise caution in applying our rules so as to avoid destroying that efficiency. In modern society we have perfected the ability to generate huge amounts of information. We must be careful that we do not inhibit the public's ability to access valuable information by immersing it in a sea of otherwise meaningless information. If DOS rules are applied too stringently, then "too many e-mail messages would be determined to be public records, clogging...system[s] with unimportant messages." E-Mail Comments, Comment No.2 at 44635. See Endnote 1. That result should be avoided.

Under DOS rules, retention periods for public records are based on the content of the record, not on the method by which a record is transmitted. See generally, Fla. Admin. Code Ch. IB-24. Current DOS rules allow for the disposition of records when the records have lost their legal, fiscal, administrative or historical value. See Fla. Admin. Code R. IB-24.004(1); see, e.g., General Records Retention Schedule For State Agencies A-I, February 1, 1993, Department of State, Division of Library and Information Services ("General Records Retention Schedule"). Consistent with that policy, the Supreme Court of Florida has established a definition of "public records" that is based on the three basic administrative purposes for which records are maintained. These purposes are the perpetuation, communication or formalization of knowledge. Shevin v. Byron, et al., 379 So. 2d 633, 640 (Fla. 1980) (" a public record is any material prepared in

connection with official agency business which is intended to perpetuate, communicate or formalize knowledge of some type. It).

Public policy dictates that DOS protect public records with legal, fiscal, administrative or historical value from destruction while assuring, for all of the reasons described above, that the use of e-mail and public access to e-mail are not inhibited by a policy that is overly protective of records with little or no value.

Records not intended to perpetuate or formalize knowledge:

As previously noted, many e-mail messages are "not prepared in connection with official agency business." Shevin, 379 So. 2d at 640. These messages do not fall within the Florida Supreme Court's definition of public records and need not be retained. Other messages are not intended to serve the administrative purposes of "perpetuating" or "formalizing" knowledge. See id. Of the three types of value identified by the Supreme Court of Florida, many e-mail messages seem to have only communicative value. In the absence of an intention to perpetuate or formalize knowledge, these messages lose their administrative value as soon as the communication takes place. Therefore, there is no logical reason to retain an e-mail message that was created without an intention to perpetuate or formalize knowledge. DOS's individual and general records schedules should allow for the disposal of such messages as soon as they have been received.

Existing agency policies:

Some agencies have already begun to follow this approach. The University of Florida's recently published Policy On Public Records Law and E-Mail ("UF Policy"), which governs records created by University of Florida personnel, explains that most e-mail falls within two categories: (1) "routine announcements and information including notices of seminars or workshops, queries regarding processes or ideas and general information regarding programs; reference files that are general-information files used in daily functions of the administrative area; and meeting notices, minutes, statistical records, reading files, and recipients' inter-department memoranda; and (2) general correspondence, sender's inter- department memoranda, and most

fiscal and budget records." Consistent with DOS rules, the UF Policy allows for the disposal of items listed in category (1) "as soon as their administrative purpose is served." Items included in category (2) must be "retained for three fiscal years."

The policy goes on to note that "retention schedules are based on a record's informational content, not its format. E-mail that falls into the category of 'retain until administrative purpose is served' may be deleted on a daily basis." The State of Connecticut has recently established a policy for e-mail messages that calls for messages of greater substance to be retained under existing guidelines. Other messages, "including copies posted to several persons and casual and routine communications similar to telephone conversations" are treated as "transitory non- record communications." (See Connecticut E-mail Policy.) Under the Connecticut policy, employees may delete these messages immediately without obtaining further approval.

Transitory e-mail messages under Florida law; recommendations: While messages of the type described in the Connecticut rule cannot be considered "non-records" under the definition established by the Supreme Court of Florida in Shevin, such messages are "transitory." These messages have only communicative value, and they lose that value upon receipt by the addressee. See Endnote 2. While e-mail messages intended to formalize or perpetuate knowledge must be retained for the time periods prescribed under current DOS rules, we should not require that records with only communicative value be retained after that value is lost. Requiring further retention of such records would be inconsistent with DOS policy that allows destruction of records that can be characterized as "obsolete, superseded or administrative value is lost." It would lead to the unnecessary retention of useless information, inhibit the use and manageability of e-mail, and limit the public's ability to access useful public records.

For these reasons, DOS should amend its general and individual records schedules by adding an additional record series called "transitory messages." This will allow agencies to dispose of transitory e-mail messages and other transitory messages without further authorization from DOS.

RETURN TO LIST OF TOPICS

CONCLUSIONS

Your questions are answered in the order in which they were asked as follows:

1. Some e-mail messages are public records.
2. The disposition of e-mail messages that are public records is governed by existing DOS rules.
3. Retention periods for e-mail messages that contain traditional information such as memoranda and correspondence are adequately covered by existing records retention schedules. However, DOS should amend these schedules to facilitate the disposition of transitory communications. DOS may also want to offer some form of non-rule guidance to other agencies and the public with regard to methods of retaining e-mail and providing public access. The UF Policy is attached as an appendix to this opinion as an example of how guidelines might be made available to agencies and the public without extensive rulemaking. See Endnote 3.

Our office proposes the following definition of "transitory messages" for your review and consideration.

RETURN TO LIST OF TOPICS

TRANSITORY MESSAGES (Item #)

This record series consists of those records that are created primarily for the communication of information, as opposed to the perpetuation or formalization of knowledge. The informal nature of transitory messages might be compared to a communication taking place during a telephone conversation, or verbal communications in an office hallway. Transitory messages are messages with short- lived administrative value and may include, but would not be limited to, many e- mail messages, telephone voice mail, many messages on "post-it" notes, and most written telephone messages.

RECOMMENDED RETENTION: Retain until obsolete, superseded, or administrative value is lost.

DLB/emiv

RETURN TO LIST OF TOPICS

ENDNOTES:

Endnote 1 -The comments to the Federal Rules also expressed concern that stringent requirements could "violate the spirit and intent of the President's National Performance Review initiative to streamline government and reduce regulations." E-Mail Comments, Comment No.1 at 44635. In Florida, we are operating under similar directives from Secretary of State Mortham and the Florida Cabinet to eliminate unnecessary rules and streamline those that remain.

GO BACK TO TEXT.

Endnote 2 -In many instances where e-mail users wish to convey substantive information or other significant thoughts, they do so by attaching a document or memorandum ("attachments") to an e-mail message. Where an e-mail user takes the additional steps necessary to create an original document or memorandum and send it as an attachment, there is a strong likelihood that the sender intended to "formalize" or "perpetuate" knowledge. Thus, attachments are less likely to be considered "transitory."

GO BACK TO TEXT.

Endnote 3 -While the UF Policy generally offers good guidance; it does not reflect the most recent revisions to the DOS rules. Therefore, the policy may be misleading on some points.

GO BACK TO TEXT.