State of Florida

ELECTRONIC RECORDS
AND
RECORDS MANAGEMENT PRACTICES

November 2010

Florida Department of State
Division of Library and Information Services

850.245.6750

http://dlis.dos.state.fl.us/RecordsManagers

What are Public Records?

Electronic records that meet the definition of a public record must be managed and made available according to applicable laws and rules. The Florida Public Records Law, Chapter 119, Florida Statutes, defines **public records** as:

> "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."

The Florida Supreme Court further interpreted the statutory definition to mean "any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type,"[1] and the courts have determined that information stored in a public agency's 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. . ."[2]

Section 119.01(2)(a), Florida Statutes, provides that "Automation of public records must not erode the right of access to those records. As each agency increases its use of and dependence on electronic recordkeeping, each agency must provide reasonable public access to records electronically maintained and must ensure that exempt or confidential records are not disclosed except as otherwise permitted by law." Therefore agencies must take steps to ensure that their electronic records are properly maintained and available when requested.

An **electronic record** is any information that is recorded in machine readable form.[3] Electronic records include numeric, graphic, audio, video, and textual information which is recorded or transmitted in analog or digital form such as electronic spreadsheets, word processing files, databases, electronic mail, instant messages, scanned images, digital photographs, and multimedia files.

An **electronic recordkeeping system** is an automated information system for the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures. [4]

[1] *Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc.*, 379 So. 2d 633 (Fla. 1980)

[2] *Seigle v. Barry*, 422 So. 2d 63, 65 (Fla.4th DCA 1982), *review denied*, 431 So. 2d 988 (Fla. 1983).

[3] Rule 1B.26.003(5)(e), *Florida Administrative Code*; Rule 1B.24.001(3)(e), *Florida Administrative Code*

[4]

Policies and Procedures

Agencies must establish policies and procedures to ensure that electronic records and their documentation are retained and accessible as long as needed. Agencies are required to include electronic records management objectives, responsibilities, and authorities in pertinent agency directives, or rules, as applicable.[5] Agencies can begin to manage their electronic records by incorporating electronic records into any general agency records management policies they may have in place. They should specify in their records management policies that those policies apply to public records in any and all formats, including electronic format, and they should ensure that employees are educated regarding these policies.

Similarly, records management requirements should be incorporated into the agency's IT policies; for instance, if the agency has an e-mail policy, it should alert users that e-mails as well as other forms of electronic communication relating to agency business are public records and are subject to all public records access, duplication, retention, and legal discovery requirements. An example of how this can be done is shown in the Department of State's internal e-mail policy in Appendix A.

Rule 1B-26.003(12), *Florida Administrative Code*, specifies that agency policies and procedures include provisions for:

> Scheduling the retention and disposition of all electronic records, as well as

Managing Electronic Records

As with records in other formats, electronic records must be managed through their entire life cycle from creation, when the records are created or received; through their active life, when the records are accessed frequently (at least once a month); through their inactive life, when the records are no longer active but have to be retained for a period of time for legal, fiscal, administrative, or historical reasons; until their final disposition which could be destruction or preservation as a permanent record.

Records Inventory

In order to know what electronic records must be managed, agencies should create an inventory or other means of identifying and locating all of their records, regardless of format, and ensure that all the records are included in approved retention schedules. The Records Inventory Sheet included in Appendix B can be used in this process.

Maintenance of Electronic Records and Media

There is often a presumption that because information is stored in the computer or on disk or tape, it is somehow automatically preserved for all time. Unfortunately, electronic storage media can easily become unreadable over time due to physical, chemical, or other deterioration. Special care and precautionary measures must be taken to avoid the loss of records stored on electronic media. Rule 1B-26.003, *Florida Administrative Code*, specifies maintenance requirements for electronic storage media.

> Preservation duplicates of permanent or long-term records must be stored in an off-site storage facility with constant temperature (below 68 degrees Fahrenheit) and relative humidity controls.
>
> Storage and handling of magnetic tape containing permanent or long-term records should conform to the magnetic tape standard AES22-1997 (r2003), "AES recommended practice for audio preservation and restoration - Storage and handling - Storage of polyest

Additional tape maintenance:

- Only rewind tapes immediately before use to restore proper tension.
- When tapes with extreme cases of degradation are discovered, they should be rewound to avoid more permanent damage and copied to new media as soon as possible.
- To ensure even packing, tapes should be played continuously from end to end.
- Tapes should be stored so that all the tape is on one reel or hub.

Environmental Controls

Electronic records media should be stored in a cool, dry, dark environment (maximum temperature 73 degrees Fahrenheit, relative humidity 20-50 percent).

Smoking, eating, and drinking must be prohibited in areas where electronic record media are recorded, stored, used, or tested.

Electronic record media must not be stored closer than 2 meters (about 6 feet, 7 inches) from sources of magnetic fields, including generators, elevators, transformers, loudspeakers, microphones, headphones, magnetic cabinet latches, and magnetized tools.

Electronic records on magnetic tape or disk must not be stored in metal containers unless the metal is non-magnetic.

Storage containers must be resistant to impact, dust intrusion, and moisture.

Compact disks must be stored in hard cases, and not in cardboard, paper, or flimsy sleeves.

Media Conversion

Agencies must 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.

Permanent or long-term electronic records stored on magnetic tape must be

Electronic Records Back-up for Disaster Recovery

> Agencies must back up electronic records on a regular basis to safeguard against loss of information due to equipment malfunctions, human error, or other disaster.
>
> Back-up media created for disaster recovery purposes must be stored in an off-site storage facility with constant temperature (below 68 degrees Fahrenheit) and relative humidity controls.

Disaster recovery back-up tapes or other media should be kept solely as a security precaution and are not intended to serve as a records retention tool. In the case of disaster, the back-up would be used to restore lost records. Agency records that have not met their retention should not be disposed of on the basis of the existence of a back-up.

If, for any reason (for instance, a disaster erases e-mails on an agency server), the only existing copy of an item that has not met its retention period is on a back-up tape or other medium, the agency must ensure that the record on the back-up is maintained for the appropriate retention period. A back-up containing record copies or the only existing copies of records that have not passed their retention would have to be retained for the length of the longest unmet retention period. Preferably, the records should be restored to an accessible storage device from the back-up to ensure that the back-up is not used as a records retention tool.

Agency IT policies should establish, and agencies should adhere to, a regular cycle of back-up overwrites based on the agency's security and disaster recovery needs.

Managing Exempt and Confidential Public Records

The Florida statutes contain hundreds of specific exemptions to the access and inspection requirements of the Public Records Law. The statutes also designate many records as exempt *and* confidential. Whether their records are designated as exempt and confidential or simply exempt, agencies are responsible for ensuring that these public records are properly safeguarded. Electronic recordkeeping systems must have appropriate security in place to protect information that is confidential or exempt from disclosure.

When providing access to or destroying electronic records containing confidential or exempt information, agencies must take steps to prevent unauthorized access to or use of the exempt information.

Retention Requirements for Electronic Records

There is no single retention period that applies to all of any agency's electronic records, or all electronic records in a particular format such as e-mail. Retention periods are determined by the content, nature, and purpose of records, and are set based on their legal, fiscal, administrative, and historical values, regardless of the format in which they reside. Records in any format can have a variety of purposes and relate to a variety of program functions and activities. The retention of any particular electronic record will generally be the same as the retention for records in any other format that document the same program function or activity.

The *General Records Schedule GS1-SL for State and Local Government Agencies*, available at http://dlis.dos.state.fl.us/recordsmgmt/gen_records_schedules.cfm, does provide the following retention requirements or guidance for certain categories of electronic records. **However, there are many other categories of records in the GS1-SL which agencies might be creating and maintaining in electronic form and agencies may also have some electronic records covered by individual schedules; be sure to use the applicable retention schedule for your records based on their nature, content, and purpose**.

AUDIT TRAILS: CRITICAL INFORMATION SYSTEMS **Item #393**

This record series consists of system-generated audit trails tracking events relating to records in critical information systems including, but not limited to, systems containing patient records, law enforcement records, public health and safety records, clinical trial records, voter and election records, and financial

GEOGRAPHIC INFORMATION SYSTEMS (GIS) SNAPSHOTS: ADMINISTRATIVE Item #382
This record series consists of periodic snapshots of Geographic Information Systems (GIS) data considered by the agency to have only short-term, administrative value. This series does not include GIS snapshots that document long-term community development and/or growth and are considered by the agency to have long-term informational and/or historical value. This series may include daily or monthly snapshots taken for general administrative or reference purposes. This series does not include snapshots taken by an agency for the sole purpose of back-up/disaster recovery. See also "GEOGRAPHIC INFORMATION SYSTEMS (GIS) SNAPSHOTS: HISTORICAL," "GEOGRAPHIC INFORMATION SYSTEMS (GIS) SOURCE DOCUMENTS/DATA," and "GEOGRAPHIC INFORMATION SYSTEMS (GIS) DATA LAYERS AND DATASETS."
RETENTION:
a) Record Copy. 1 anniversary year.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

GEOGRAPHIC INFORMATION SYSTEMS (GIS) SNAPSHOTS: HISTORICAL Item #383
This record series consists of periodic snapshots of Geographic Information Systems (GIS) data considered by the agency to have long-term informational and/or historical value. This series may include, but is not limited to, snapshots documenting community development and/or growth such as geographic contour changes; infrastructure development, including transportation, utilities, and communications; environmental changes; demographic shifts; changes to jurisdictional boundaries; and changes in property values. This record series does not include GIS snapshots taken by an agency for the sole purpose of back-up/disaster or snapshots taken for general administrative or reference purposes such as documentation of routine infrastructure maintenance (e.g., road repairs, utility line repairs). See also "GEOGRAPHIC INFORMATION SYSTEMS (GIS) SNAPSHOTS: ADMINISTRATIVE," "GEOGRAPHIC INFORMATION SYSTEMS (GIS) DATA LAYERS AND DATASETS," and "GEOGRAPHIC INFORMATION SYSTEMS (GIS) SOURCE DOCUMENTS/DATA." These records may have archival value.
RETENTION:
a) Record Copy. **Permanent.** State agencies should contact the State Archives of Florida for archival review after 5 years. Other agencies should ensure appropriate preservation of records.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

GEOGRAPHIC INFORMATION SYSTEMS (GIS) SOURCE DOCUMENTS/DATA Item #384
This record series consists of documents and/or data used to update Geographic Information Systems (GIS). This record series may include, but is not limited to, address change forms, survey data, field notes, legal descriptions, and other documents and/or data submitted to or acquired by the agency for the sole purpose of updating the agency's Geographic Information Systems. Do NOT use this item if records fall under a more appropriate retention schedule item or if the unique content/requirements of the records necessitate that an individual retention schedule be established. See also "GEOGRAPHIC INFORMATION SYSTEMS (GIS) DATA LAYERS AND DATASETS," "GEOGRAPHIC INFORMATION SYSTEMS (GIS) SNAPSHOTS: ADMINISTRATIVE," and "GEOGRAPHIC INFORMATION SYSTEMS (GIS) SNAPSHOTS: HISTORICAL."
RETENTION:
a) Record Copy. Retain until obsolete, superseded, or administrative value is lost.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

SPAM/JUNK ELECTRONIC MAIL JOURNALING RECORDS Item #370
This record series consists of electronic mail items identified by an agency's filtering system as spam or junk mail that are blocked from entering users' mailboxes and instead are journaled, or captured as an audit log along with their associated tracking information, as evidence of illegal acts. The journaling records lose their value within a brief period after their capture unless it is determined that they should be forwarded to a law enforcement agency for investigation.
RETENTION:
a) Record copy. Retain until obsolete, superseded, or administrative value is lost.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

Destruction of Electronic Records

Rule 1B-24, *Florida Administrative Code*, sets forth requirements for destruction of public records. Section (10) of the rule specifies the following:

> Agencies must ensure that all destruction of records is conducted in a manner that safeguards the interests of the state and the safety, security, and privacy of individuals.
>
> In destroying records containing information that is confidential or exempt from disclosure, agencies must use destruction methods that prevent unauthorized access to or use of the information and ensure that the information cannot practicably be read, reconstructed, or recovered.
>
> Agencies must specify the manner of destruction of such records when documenting disposition.
>
> When possible, recycling following destruction is encouraged.
>
> For electronic records containing information that is confidential or exempt from disclosure, appropriate destruction methods include physical destruction of storage media such as by shredding, crushing, or incineration; high-level overwriting that renders the data unrecoverable; or degaussing/demagnetizing.

Many commercial shredding companies offer shredding services for electronic storage media such as compact disks and DVDs.

Transitory messages are not intended to formalize or perpetuate knowledge and do not set applications typically require little to no action on the part of the user to store the e-mail records. Once messages are stored, authorized users are able to search the repository.

In the archiving process, e-mail may be removed from the mail server either manually by the user or automatically after a predetermined period of time. Automatic transfer to the e-mail archive server may be based on a characteristic or combination of characteristics explicitly found in the e-mail such as the identity of the sender or recipient, date, or keywords found in the subject line or text of the message. The archive server then indexes the e-mail and associated files for future search and retrieval. E-mail systems continue to provide access to archived e-mail through pointers or shortcuts. In most situations, only one copy of the e-mail gets archived.

Recordkeeping systems that include electronic mail messages, including e-mail archiving systems being used to store record copy emails, must:

> Provide for the grouping of related records into classifications according to the business purposes the records serve;
>
> Permit easy and timely retrieval of both individual records and files or other groupings of related records;
>
> Retain the records in a usable format for their required retention period and allow their disposal when the retention is met;
>
> Be accessible by individuals who have a business need for information in the system;
>
> Preserve the transmission and receipt data specified in agency instructions.

Depending on the agency and its business purposes, e-mail archiving applications may provide the following benefits. Each application has different features and different strengths, so this list is not exhaustive:

> More efficient storage of e-mail because it is moved from a distributed network of servers, desktop applications, and other places to be managed in one place;
>
> Enhanced electronic search capability for content that may be germane to a subpoena, public records request, e-discovery request, or similar purpose;
>
> Back-up and disaster recovery features.

While e-mail archiving applications offer business benefits, these technologies do not necessarily meet all of the requirements of the public records laws and rules. Unless the agency appropriately configures and implements the application, it can weaken a records management program. For instance:

Cloud Computing

Cloud computing is a term that refers to accessing via the Internet computer resources that are owned and operated by a service provider in one or more data center locations. Cloud computing customers use resources as a service and pay only for resources that they use, thereby avoiding capital expenditu

Security – There is debate as to whether or not cloud services provide more or less security than traditional IT infrastructure. Some argue that data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security.

For agencies considering deploying cloud computing services, it will be important to address these issues and others like them upfront. **Have the provider demonstrate or describe in detail how they can meet all agency requirements, and clearly delineate those requirements in the contract with the provider.**

Creating Electronic Records / Implementing Automated Systems

When creating electronic records and implementing automated systems that will contain public records, agencies must take steps to ensure the records are maintained according to applicable public records laws and rules.

Conduct a Cost Benefit Analysis

Electronic recordkeeping systems containing public records must maintain the records in accordance with applicable public

Telephone "hotlines" or "help desks" staffed by knowledgeable computer support professionals within the agency who can answer technical questions and provide "quick fix" solutions. This process may not be an adequate learning tool for good records management unless the computer support professionals have received specialized records management training.

Training offered by the manufacturer or vendor. This usually covers the operation of computer hardware and software but does not include records management concepts.

Essential Characteristics of Electronic Records and Legal Admissibility

Managing and preserving electronic records can be challenging since they are easily revised, deleted, changed, and manipulated. If appropriate measures are not taken, the essential characteristics of records can be altered or lost in the preservation process. Careful planning and system design are required to guarantee that the essential characteristics of electronic records are both captured and maintained for the lifetime of the record.

The essential characteristics of electronic records are:

Content - Information in the record that documents government business. Content can be composed of numbers, text, symbols, data, images or sound. The information content of a record should be an accurate reflection of a particular business transaction or activity.

Context - Information that shows how the record is related to the business of the agency and other records. Contextual information is crucial to the evidentiary function of records. If a record lacks key information about its creator, the time of its creation, or its relationship to other records, its value as a record is severely diminished or lost entirely.

Structure – Appearance and arrangement of a record’s content and technical characteristics of the record (e.g., file format, data organization, relationship between fields, page layout, style, fonts, page and paragraph breaks, hyperlinks, headers, footnotes). It is easier to preserve a record over time if it has a simple record structure. It is also advisable to base record structure on open standards to avoid dependence on a specific company or organization.

In order for records to serve as evidence, these three essential characteristics must be maintained. Whenever one of the characteristics is altered, the ability of records to accurately reflect the activities of an agency is diminished.

Legal admissibility concerns whether a piece of evidence would be accepted by a court of law. If a record does not hold evidential weight, it could potentially harm a case being fought. If the authenticity and accuracy of the records can be demonstrated then they will have evidential weight. There are two main elements that demonstrate authenticity of electronic records:

The system's ability to "freeze" a record at a specific moment in time; and

Maintenance of a documented audit trail.

File Format (TIFF) and Portable Document Format (PDF) are examples of formats based on a publicly available, authoritative specification for scanned images.

Widespread Adoption and Use - Formats adopted for widespread use have a higher probability of being sustainable over time. When a format has been widely adopted by users, multiple software tools are created to open, read, and access the records and the market supports ongoing sustainability of the file format. This extends the time that the information can be maintained in the format using readily-available tools. The adoption of a file format by information creators, disseminators, and users is an indicator of sustainability. Hyper-text Markup Language (HTML) is an example of a format that has been widely adopted for Internet use.

Self-describing Formats - Self-describing formats contain metadata needed to interpret the content, context, and/or structure of the record. Metadata embedded within the format minimizes reliance on external documentation and the risk of disassociation of metadata from the file over time. While self-describing formats provide the capability for including metadata (e.g., in the file header or through tags within the file structure), they may not necessarily mandate it in the format specification. If present, the metadata should be easily accessed. This ensures that descriptive information about the record is sustainable. Extensible Markup Language (XML) is an example of a self-documenting format because it describes its structure and field names.

When agencies use formats that exhibit these characteristics, they increase the likelihood that the information will be accessible over the long term.

When creating electronic records or converting source data, agencies can enhance sustainability by maintaining the original quality of source data. The following methods are typically applied through software settings and vary depending on the format being used.

Technical Protection Mechanisms - Long-term records should be unrestricted and/or unencrypted so that user IDs and/or passwords are not needed to maintain the file. User IDs and passwords can be lost over time.

Maintain Integrity of Source Data - When using compression to reduce file size, agencies should use lossless compression to maintain the integrity of source data. Lossless compression produces smaller file sizes without removing any information. Maintaining the original quality of source data can facilitate future migration and conversion. Minimizing subsequent modification of the records after production is also recommended to maintain integrity.

While selecting appropriate formats does not guarantee sustainability, it does significantly increase the probability that those records will remain accessible and readable for as long as necessary. Of course, agencies need to follow other record

> A scanning density with a minimum of 300 dots per inch (dpi) is required for scanned images created by the agency from hard copy permanent or long-term records.
>
> Record (master) copies of scanned images created by the agency from hard copy permanent or long-term records must be in accordance with a published International Organization for Standardization (ISO) open standard image format. Published standards can be found at http://www.iso.org/iso/home.htm. There is no specific image format requirement for records with a retention of less than 10 years, although the agency must ensure that the records remain accessible and readable for as long as they are retained.

Using CDs and DVDs for Storage

CDs and DVDs are not recommended for storing the record copy of permanent or long-term records. If you choose to use CDs and DVDs for storing short-term records, you should understand their properties and limitations.

Compact Disk-Read Only Memory (CD-ROM) is a type of optical disk capable of storing up to 1GB (gigabyte) of data - although the most common size is 650MB (megabytes). A single CD-ROM has enough memory to store about 300,000 text pages.[8]

Digital Versatile Disk or Digital Video Disk (DVD) is a type of optical disk technology similar to the CD-ROM. A DVD holds a minimum of 4.7GB of data with enough memory for a full-length movie. DVDs are commonly used as a medium for digital representation of movies and other multimedia presentations that combine sound with graphics.[9]

CD-R stands for CD-Recordable; DVD-R stands for DVD-Recordable. With CD-R/DVD-R, data can be recorded once, after which the disk becomes read-only. Use only CD-R/DVD-R disks for storing short-term records. These disks provide protection for your records against tampering or loss of data.

CD-RW/DVD-RW stands for CD Re-Writable or DVD Re-Writable. Rewritable media are not appropriate for electronic records storage or retention. RW disks can be written to multiple times. The film layer on RW disks degrades at a faster rate than the dye used in CD-R/DVD-R disks, especially with frequent recording and re-writing.

CD and DVD media often support multiple logical and physical formats that determine the hardware and software that will be required to read from the disks in the future. For example, Apple computers can read and write CDs in the HFS+ logical format while PCs running Microsoft Windows operating systems usually read and write CDs using the ISO 9660 logical format with Joliet extensions.

[8] www.webopedia.com.
[9] www.webopedia.com.

The color of a CD/DVD indicates its quality. It is best to look for a gold or silver CD/DVD; look at the color from the underside of the disk, not the top. In addition, to assure the highest quality of a CD-R, look for those manufactured using phthalocyanine dye with gold or silver reflective layers. Do not use Azo- or (plain) cyanine-dyed media. For DVD-Rs, purchase double-sided/single-layer with a gold reflective underside. To assure you're using the highest quality CD/DVD and/or to avoid pitfalls in purchasing the correct type, refer to the source references below (page 33).

It is best to purchase new CDs/DVDs as they are needed. According to the Optical Storage Technology Association (OSTA), the unrecorded shelf life of a CD-R/DVD-R disk is conservatively estimated to be between 5 and 10 years.[10]

CD/DVD experiential life expectancy is 2 to 5 years even though published life

CDs and DVDs and their containers should be labeled so that they can be identified and organized according to your inventory. Many vendors sell CD-safe markers. For risk-free labeling of any disk, it is best to mark the clear inner hub or the so-called mirror band of the disk where they contain no data. Do not apply adhesive labels to the CD/DVD because they can damage the disk.

Disks are best stored upright (like a book) in "jewel" cases that are designed specifically for CDs/DVDs. Ideally, store the cases in plastic or steel containers manufactured specifically for the type of medium in cool, dry storage that is free of large temperature fluctuations. Generally, useful life will be increased by storing disks at a low temperature and low relative humidity, since chemical degradation is reduced in these conditions. Store at 62-70 degrees Fahrenheit and 35-50% relative humidity. Daily fluctuations in the storage area should not exceed +/- 2 degrees Fahrenheit in temperature or +/- 5% in relative humidity.

When short-term records reach the end of their retention period, or if damage occurs to media while in storage, you will want to ensure that the data are irretrievable. See section on **Destruction of Electronic Records** (page 13).

The following sources provide additional resources and publications on electronic storage media:

NIST Special Publication 500-252, "Information Technology: Care and Handling of CDs and DVDs: A Guide for Librarians and Archivists," published by the U.S. Department of Commerce, National Institute of Standards and Technology (http://www.itl.nist.gov/iad/894.05/docs/CDandDVDCareandHandlingGuide.pdf);

Digital Preservation Guidance Note: "Care, Handling and Storage of Removable Media," from United Kingdom Digital Preservation Department of The National Archives (http://www.nationalarchives.gov.uk/documents/media_care.pdf);

"Using CDs for Data Storage," from the School of Library, Archival, and Information Studies, University of British Columbia, Canada (http://www.slais.ubc.ca/PEOPLE/students/student-projects/C_Hill/hill_libr516/index.htm);

Professional organizations such as the Association of Records Managers and Administrators (ARMA, www.arma.org), and the Association of Image and Information Management (AIIM, www.aiim.org);

The Optical Storage Technology Association (OSTA, http://www.osta.org/); and Report: "Relative Stabilities of Optical Disk Formats," Joe Iraci, in the Restaurator - International Journal for the Preservation of Library and Archival Material (2005) (

File Naming

Managing electronic files can be overwhelming if there is no organized method for naming and storing files. Efficient electronic filing practices help to ensure that files can be retrieved quickly and with the lowest possible cost.

File naming is an important part of managing any system of records. A file name is the principal identifier for a record. Having a unified naming system can help place records in context with other records as well as associated record series and retention schedules. Records that are named using a consistent, logical system can be more easily located and shared among users. Agencies may want to consider an agency-wide file naming policy as part of their strategy for managing electronic records.

When developing a file naming policy, consider including as part of the file name some of the following common conventions:

> Version number (e.g., version 1 [v1, vers1])
>
> Date of creation (e.g., April 14, 2010 [04142010, 04_14_2010])
>
> Name of creator (e.g., Edward N. Johnson [ENJohnson, ENJ])
>
> Description of content (e.g., media kit [medkit, mk])
>
> Name of intended audience (e.g., general public [pub])
>
> Name of group associated with the record (e.g., Committee ABC [CommABC])
>
> Release date (e.g., released on March 24, 2008 at 10:30 a.m. eastern time [03242008_1030ET])
>
> Publication date (e.g., published on December 31, 2009 [pub12312009])
>
> Project number (e.g., project number 625 [PN625])
>
> Department number (e.g., Department 126 [Dept126])
>
> Records series (e.g., Series2036)

The following issues should also be considered when developing a file naming policy:

> Access and ease of use. The policy should be simple and straightforward. A simple policy will help staff members logically and easily name records and help ensure that records are accessible to staff members and/or to the public. A simple policy will be more consistently used, resulting in records that are consistently named and thus easier to organize and access.

Electronic Document Management Systems (EDMS) are also widely used in organizations to control the creation, use, and destruction of electronic documents to facilitate workflow. EDMS often lack some of the functionality needed to fully manage records but support such functions as indexing of documents, storage management, version control, close integration with desktop applications, and retrieval tools to access the documents.

Some systems, known as Electronic Document and Records Management Systems (EDRMS), combine ERMS and EDMS functionality into one integrated system. The chart below compares EDMS and ERMS features and shows important distinctions between them.

An EDMS…	An ERMS…
• allows documents to be modified and/or to exist in several versions; • may allow documents to be deleted by their owners; • may include some retention controls; • may include a document	

managing electronic records. This document is very readable and has practical advice for evaluating and selecting these systems. It is available at http://ec.europa.eu/transparency/archival_policy/moreq/doc/moreq2_spec.pdf.

PIN, etc), multimedia messaging (such as MMS), chat messaging, social networking (such as Facebook, Twitter, etc.), or any other current or future electronic messaging technology or device. Retention periods are determined by the content, nature, and purpose of records, and are set based on their legal, fiscal, administrative, and historical values, regardless of the format in which they reside or the method by which they are transmitted. Electronic communications, as with records in other formats, can have a variety of purposes and relate to a variety of program functions and activities. The retention of any particular electronic message will be the same as the retention for records in any other format that document the same program function or activity. For instance, electronic communications might fall under a CORRESPONDENCE series, a BUDGET RECORDS series, or one of numerous other series, depending on the content, nature, and purpose of each message. Electronic communications that are created primarily to communicate information of short-term value, such as messages reminding employees about scheduled meetings or appointments, might fall under the "TRANSITORY MESSAGES" series.

The retention requirements are based on the nature, content, and purpose of the records and not on the physical format in which they exist.

4. If we print out our e-mail messages, do we also have to keep them in electronic form?

Printouts of e-mail files are acceptable in place of the electronic files provided that the printed version contains all date/time stamps, routing information, etc. This information usually prints automatically at the top of each printed e-mail and includes name of the sender, names of all recipients (including To, CC, and BCC), date/time sent or received, subject line, and an indication if an attachment was present (attachments should be printed and retained with the printed e-mail). This can be applied broadly to other types of electronic records that you are going to print and retain only in paper form. Any metadata that is necessary to understanding the nature and content of the record should be printed along with the record.

However, as indicated in the

when the content of the posting or comment satisfies the definition of “public record” in section 119.011(12), Fla. Stat. (2008). . . those comments whose content falls within the definition of public record must be retained by agencies in accordance with the appropriate Division retention schedules.”

If you post a copy of a public record (such as the minutes of a meeting) to a website or social networking site, it is not necessary to maintain that Web copy indefinitely as long as you retain the record copy in your office in accordance with the applicable retention schedule.

government-owned computer system. However, if the Department discovers misuse of the e-mail system, personal e-mails that are identified as being in violation of Department policy may become public record as part of an investigation.

c. The Florida Statutes contain numerous specific exemptions to the access and inspection requirements of the Public Records Law. Employees are responsible for ensuring that electronic public records which are exempt from access or inspection by statute are properly safeguarded.

6. Use of E-Mail System

a. The Department's e-mail system is to be used to conduct official Department business and is not to be used for any other purpose unless expressly approved by authorized Department officials. E-mail may be used to communicate with Department staff and with other public and private entities to conduct official Department business.

b. Incidental, personal use of the e-mail system is permitted; however, the personal use must be brief, must not interfere with the employee's work or the work of others, must not subject the Department to any additional cost, and must not be prohibited by this policy or any federal, state or local law, statute, ordinance, rule or regulation.

7. Prohibited Uses of E-Mail

The Department's e-mail system shall not be used for any unauthorized purpose including, but not limited to:

a. Sending solicitations including, but not limited to, advertising the sale of goods or services or other commercial activities, which have not been approved by the Department.

b. Sending copies of documents in violation of copyright laws or licensing agreements.

c. Sending information or material prohibited or restricted by government security laws or regulations.

d. Sending information or material which may reflect unfavorably on the Department or adversely affect the Department’s ability to carry out its mission.

e. Sending information or material which may be perceived as representing the Department’s official position on any matter when authority to disseminate such information has not been expressly granted.

f. Sending confidential or proprietary information or data to persons not authorized to receive such information, either within or outside the Department.

g. Sending messages or requesting information or material that is *fraudulent, harassing, obscene, offensive, discriminatory, lewd, sexually suggestive, sexually explicit*, *pornographic,*

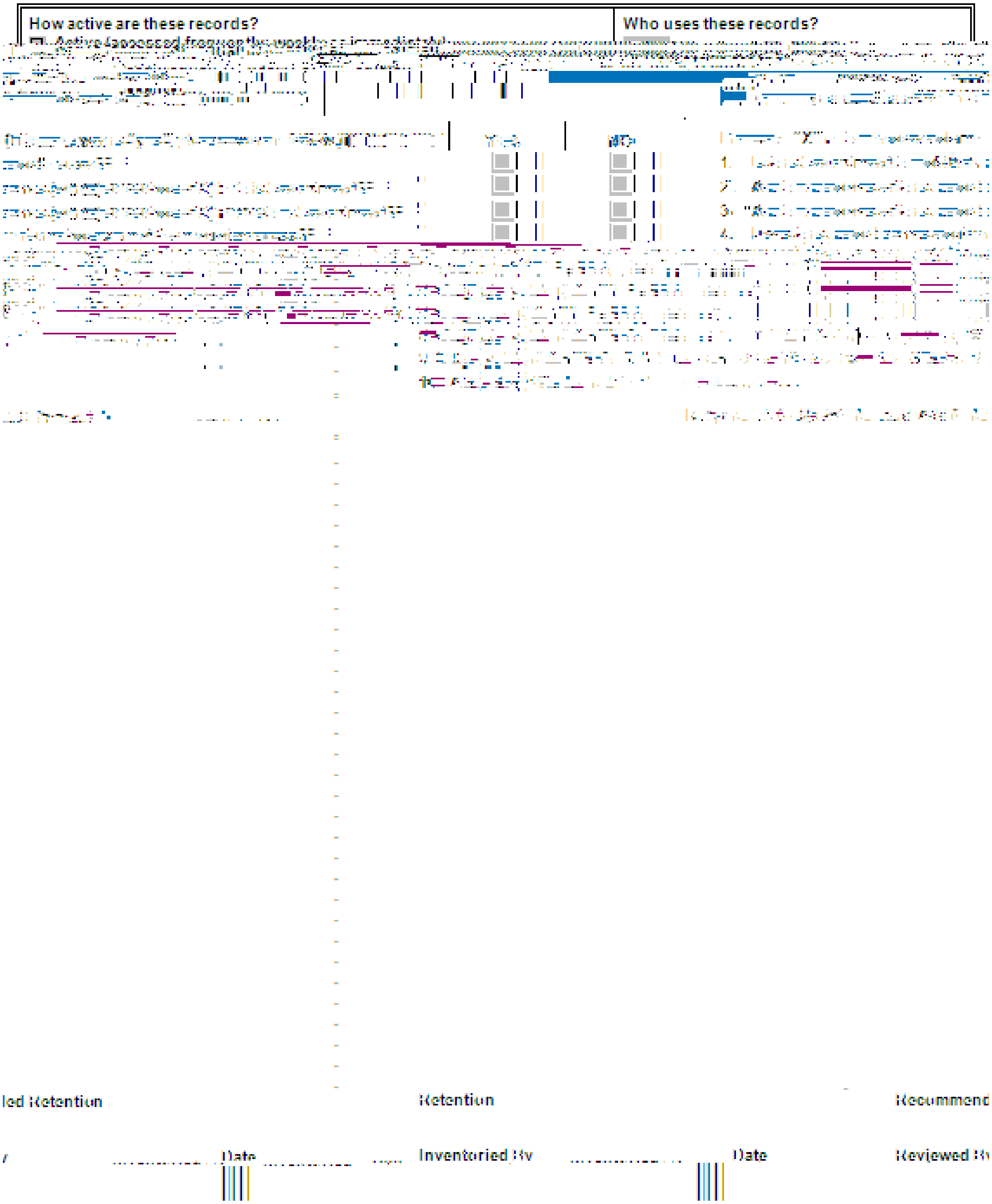
Department of State Policies and Procedure
Electronic Mail Policy
Page 4 of 4

10. Transitory Messages

Many, though not all, e-mails fall under the retention schedule for "TRANSITORY MESSAGES" (General Records Schedule GS1-SL for State and Local Government Agencies, Item #146). "Transitory Messages" are messages that do not set policy, establish guidelines or procedures, certify a transaction or become a receipt. Cc -Messages

APPENDIX B - Records Inventory Worksheet

Fillable Worksheet form in Word format available at http://dlis.dos.state.fl.us/recordsmgmt/publications.cfm.



How active are these records?

□ Active (accessed frequently: weekly ... immediately)

Who uses these records?

Yes

No

1.

2.

3.

4.

led Retention

Retention

Recommend

Date

Inventoried By

Date

Reviewed By

APPENDIX C - Rule 1B-26.003 Florida Administrative Code

1B-26.003 Electronic Recordkeeping.

(1) PURPOSE. These rules provide standards for record (master) copies of public records which reside in electronic recordkeeping systems. Recordkeeping requirements must be incorporated in the system design and implementation of new systems and enhancements to existing systems. Public records are those as defined by Section 119.011(11), F.S.

(2) AUTHORITY. The authority for the establishment of this rule is Sections 257.14 and 257.36(1) and (6), F.S.

(3) SCOPE.
(a)1. These rules are applicable to all agencies as defined by Section 119.011(2), F.S.
2. These rules establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposition of electronic record (master) copies, regardless of the media.
3. Electronic records include numeric, graphic, audio, video, and textual information which is recorded or transmitted in analog or digital form.
4. These rules apply to all electronic recordkeeping systems, including, but not limited to, microcomputers, minicomputers, main-frame computers, and image recording systems (regardless of storage media) in network or stand-alone configurations.
(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.

(4) INTENT. Electronic recordkeeping systems in use at the effective date of this rule, that are not in compliance with the 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:

APPENDIX C

information associated with a database management system including a description of the relationship between data elements in databases;
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. Electronic recordkeeping systems that maintain record (master) copies of public records on electronic media shall meet the following minimum requirements:
(a)1. Provide a method for all authorized users of the system to retrieve desired records;
2. 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

(b) Retain the records in a usable format until their authorized disposition and, when appropriate, meet the

4. Software in use at the time of creation.

(g) STANDARD. For all media used to store permanent or long-term electronic records, agencies shall maintain human readable information specifying recording methods, formats, languages, dependencies, and schema sufficient to ensure continued access to, and intellectual control over, the records. Additionally, the following information shall be maintained for each media used to store permanent or long-term electronic records:
1. File title;
2. Dates of creation;
3. Dates of coverage; and
4. Character code/software dependency.
(h) STANDARD. Electronic records shall not be stored closer than 2 meters (about 6 feet, 7 inches) 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) 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.
(l) 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. Permanent or long-term 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.

(12) RETENTION OF ELECTRONIC RECORDS. Each agency is responsible for ensuring the continued accessibility and readability of public records throughout their entire life cycle regardless of the format or media in which the records are maintained. Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained and accessible as long as needed. These procedures shall 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 1B-24, F.A.C.
(b) 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.