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

Table of Contents

What are Public Records? 4
Public Records Management, Responsibilities, and Requirements 5
Policies and Procedures 7
Managing Electronic Records 8
Records Inventory 8
Maintenance of Electronic Records and Media 8
Environmental Controls 9
Media Conversion 9
Managing Exempt and Confidential Public Records 10
Retention Requirements for Electronic Records 10
Destruction of Electronic Records 14
Electronic Communications as Public Records 15
Retention Requirements for Electronic Communications 15
E-mail Archiving 16
E-Discovery 19
Cloud Computing 22
Creating Electronic Records / Implementing Automated Systems 24
Conduct a Cost Benefit Analysis 24
Incorporate Recordkeeping Requirements into System Design 24
Document Electronic Recordkeeping Systems 25
Provide Training for Users of Electronic Records 26
Essential Characteristics of Electronic Records and Legal Admissibility 27
Sustainable Formats 28
Selecting Storage Media 30
Using CDs and DVDs for Storage 31
File Naming 34
Automated Systems to Manage Electronic Records 35
Frequently Asked Questions (FAQ) 38
1. What are the requirements for scanning public records? 38
2. If I scan my records, can I get rid of the original hard copy? 38
3. How long do we have to keep our e-mail? 38
4. If we print out our e-mail messages, do we also have to keep them in electronic form? 39
5. How long do we have to keep our back-ups? Should we keep e-mail back-ups permanently in case they are ever needed? 39
6. Are postings or messages on our website, Facebook page, or Twitter site public records? If so, how long do we have to keep them? 40
7. What are Florida's requirements for electronic signatures? 41
APPENDIX A - Department of State E-Mail Policy 43
APPENDIX B - Records Inventory Worksheet 47
APPENDIX C - Rule 1B-26.003 Florida Administrative Code 49

Preface

The goal of Florida's Records Management Program is to provide professional assistance to state and local government agencies in managing the records and information required to take care of the business of government in an effective and cost-efficient manner. This is a particularly challenging goal in the 21st century. Florida public agencies generate and process information on an unprecedented scale, hastened by the rapid advance of technology. This results in vast quantities of information and evolving principles of law governing the legality and admissibility of records created or maintained by this technology. As records and information managers, we must make every effort to keep ourselves educated and informed so that the decisions we make are consistent with law and best practices.

Florida public agencies are faced with yet another challenge. Not only must we control costs through the application of sound records and information management principles, but we must also apply these principles in light of the public's right to know. Chapter 119, Florida Statutes, Florida's Public Records Law, is one of the most open public records laws in the country and a model for other states. Florida has had some form of a public records law since 1909 and is recognized nationally for its leadership regarding public records and accessibility to public information. As we go about our business, we must remember the dual responsibility we have as public records and information managers: to reduce government agencies' costs of doing business and to guarantee the public's right to know what their government is doing.

This handbook is intended to assist the creators and users of electronic records, information technology (IT) staff, records management (RM) staff, and agency managers in managing electronic records in an effective, cost-efficient manner that also accommodates their public records responsibilities. The handbook emphasizes the crucial role of records maintenance and disposition in managing electronic records and is designed to be used in conjunction with the Department of State's *Basics of Records Management* handbook. Available at http://dlis.dos.state.fl.us/barm/handbooks/basics.pdf, *Basics* provides an introduction and guide to public records management in Florida for state and local government agencies. The principals in the *Basics* handbook apply equally to public records in electronic format.

While the recommendations in this handbook reflect best practices, they are not meant to define mandatory standards. Rule 1B-26.003, *Florida Administrative Code*, provides standards for record (master) copies of public records which reside in electronic recordkeeping systems, establishes minimum requirements for the creation, utilization, maintenance, retention, preservation, storage, and disposition of electronic record (master) copies, regardless of the media, and must be followed by all agencies as defined by Section 119.011(2), Florida Statutes.

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] Rule 1B-26.003(5)(f), *Florida Administrative Code*

Public Records Management, Responsibilities, and Requirements

Chapter 119, Florida Statutes, defines "custodian of public records" as “the elected or appointed state, county, or municipal officer charged with the responsibility of maintaining the office having public records, or his or her designee.” Responsibility for properly maintaining public records, including electronic records, begins with the head of the agency. Elected or appointed officials may designate others with this responsibility but, if records are not available when they should be, it is the agency head who ultimately will have to answer for it. It is, therefore, in the agency’s best interest to support the proper management of its public records.

Agencies have a variety of public records responsibilities under Florida statute and administrative rule. Specifically:

- Chapter 119, Florida Statutes, requires records custodians to allow inspection and copying of public records except for those specifically confidential or exempt from inspection by statute.

- Chapter 257, Florida Statutes, requires agencies to establish and maintain an active and continuing program for the economical and efficient management of records.

- Chapters 119 and 257, Florida Statutes, as well as Rule 1B-24, *Florida Administrative Code*, require that agencies adhere to records retention schedules established by the Division of Library and Information Services of the Department of State and prohibit destruction of public records except in accordance with those retention schedules.

- Agencies are further required to appoint a Records Management Liaison Officer (RMLO), to submit to the Division of Library and Information Services an annual records management compliance statement, and to document disposition of their public records (Chapter 257, Florida Statutes, and Rule 1B-24, *Florida Administrative Code*).

These requirements apply to public records in all formats, including records created and/or maintained in electronic format. The complex characteristics of electronic records, and the rapid changes in the hardware and software used to access them, make these requirements even more challenging; as a result, electronic records are typically not as well managed as records in other formats. The massive quantities of electronic records make it even more difficult to manage them effectively.

Therefore, it is critical for agencies to establish a program for the management of electronic records that incorporates the program elements necessary to meet public records requirements. These program elements include:

- Administering an agency-wide program for the management of records created, received, maintained, used or stored on electronic media.
- Ensuring that all electronic records are covered by records retention schedules.
- Integrating the management of electronic records with other records and information resources management programs of the agency.
- Incorporating electronic records management objectives, responsibilities, and authorities in agency directives.
- Establishing procedures for addressing electronic records management requirements, including recordkeeping requirements and disposition.
- Ensuring that agency electronic recordkeeping systems meet state requirements for public access to records.
- Providing an appropriate level of security to ensure the integrity of electronic records.
- Ensuring that training is provided for users of electronic records systems in the operation, care, and handling of the equipment, software, and media used in the system.
- Ensuring the development and maintenance of up-to-date documentation about all electronic records systems that is adequate to specify all technical characteristics necessary for reading or processing the records and for the timely, authorized disposition of records.
- Specifying the location and media on which electronic records are maintained to meet retention requirements and maintaining inventories of electronic records systems to facilitate disposition.
- Ensuring the continued accessibility and readability of electronic records throughout their life cycle.

Successfully implementing these program elements requires a coordinated effort within the agency. The effort needs support of the agency head and other management and requires the expertise of the agency RMLO and other RM staff, IT staff, legal staff, and records custodians. IT plays a vital role in maintaining electronic records as they create and maintain the infrastructure on which the records reside. It is important for key staff to work together to ensure that electronic information is available, preserved, and disposed of according to applicable laws and rules.

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 related access documentation and indexes, in accordance with the provisions of Rule 1B-24, *Florida Administrative Code*.
- 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.
- Transferring a copy of the electronic records and any related documentation and indexes to the State Archives of Florida at the time specified in the records retention schedule, if applicable.
- Destruction of electronic records. Electronic records may be destroyed only in accordance with the provisions of Rule 1B-24, *Florida Administrative Code*. At a minimum each agency shall ensure that:

    - Electronic records scheduled for destruction are disposed of in a manner that ensures that any information that is confidential or exempt from disclosure, including proprietary, or security information, cannot practicably be read or reconstructed, and;

    - Recording media previously used for electronic records containing information that is confidential or exempt from disclosure, including proprietary or security information, are not reused if the previously recorded information can be compromised in any way by reuse.

[5] Rule 1B-26.003(6), *Florida Administrative Code*

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 polyester-base magnetic tape," available from the Audio Engineering Society, Incorporated, 60 East 42nd Street, Room 2520, New York, New York, 10165-2520, and at the Internet Uniform Resource Locator: http://www.aes.org/publications/standards/search.cfm.

- Agencies must annually read a statistical sample of all electronic media containing permanent or long-term records to identify any loss of information and to discover and correct the cause of data loss.

- Agencies must test all permanent or long-term electronic records at least every 10 years and verify that the media are free of permanent errors. More frequent testing (e.g., at least every 5 years) is highly recommended.

- 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 transferred to new media as needed to prevent loss of information due to changing technology or deterioration of storage media.

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 transaction records. Audit trails link to specific records in a system and track such information as the user, date and time of event, and type of event (data added, modified, deleted, etc.). Since audit trails may play an integral part in prosecution, disciplinary actions, or audits or other reviews, agencies are responsible for ensuring that internal management policies are in place for retaining audit trails as long as necessary for these purposes.
RETENTION:
a) Record copy. Retain each audit trail entry as long as the record the entry relates to, provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

AUDIT TRAILS: ROUTINE ADMINISTRATIVE INFORMATION SYSTEMS **Item #394**
This record series consists of system-generated audit trails tracking events relating to records in information systems used for routine agency administrative activities. Audit trails link to specific records in a system and track such information as the user, date and time of event, and type of event (data added, modified, deleted, etc.). Since audit trails may play an integral part in prosecution, disciplinary actions, or audits or other reviews, agencies are responsible for ensuring that internal management policies are in place for retaining audit trails as long as necessary for these purposes.
RETENTION:
a) Record copy. Retain until obsolete, superseded, or administrative value is lost, provided applicable audits have been released.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

BACK-UP TAPES
There is no retention schedule for back-up tapes or other forms of data back-up. A back-up tape or drive should be just that: a data/records back-up kept solely as a security precaution but ***not intended to serve as the record copy or as a records retention tool.*** In the case of disaster, the back-up would be used to restore lost records; otherwise, 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 your server) the only existing copy of an item that has not met its retention period is on a back-up tape or drive, the custodial agency of that record must ensure that the record on the back-up is maintained for the appropriate retention period. A back-up containing record copies/only existing copies of items 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 the agency from the back-up to ensure that the back-up is not used as a records retention tool.

COMPUTER LOGS **Item #391**
This record series consists of firewall logs, system logs, network logs, or other logs used to maintain the integrity and security of the agency's computer systems. The logs may record such information as source and destination Internet Protocol (IP) addresses; user identification information; files, directories, and data that have been accessed; user rights; and running applications and databases. Since these logs may play an integral part in prosecution or disciplinary actions, agencies are responsible for

ensuring that internal management policies are in place establishing criteria for which logs or entries should be retained for further investigation.

RETENTION:

a) Record copy. 30 days or until review of logs is complete, whichever occurs first.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

ELECTRONIC COMMUNICATIONS

There is no single retention period that applies to all electronic messages or communications, whether they are sent by e-mail, instant messaging, text messaging (such as SMS, Blackberry 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 generally 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.

ELECTRONIC RECORDS SOFTWARE AND DOCUMENTATION **Item #231**

This record series consists of proprietary and non-proprietary software as well as related documentation that provides information about the content, structure, and technical specifications of computer systems necessary for retrieving information retained in machine-readable format. These records may be necessary for an audit process.

RETENTION:

a) Record copy. Retain as long as software-dependent records are retained.
b) Duplicates. Retain until obsolete, superseded, or administrative value is lost.

GEOGRAPHIC INFORMATION SYSTEMS (GIS) DATA LAYERS AND DATASETS **Item #381**

This record series consists of individual layers of data and/or datasets used to populate Geographic Information Systems (GIS). Data layers and datasets may include, but are not limited to, vector data, such as point, line, and polygon data; imagery data, such as satellite imagery and aerial imagery; topographic data, including elevation data and terrain contours; land use and planning data, including habitat data, road data, zoning, and parcel ownership; and jurisdictional boundary data, including political subdivisions, historic districts, school districts, and urban growth areas. Since GIS data layers and datasets are continuously updated, agencies should take periodic snapshots of data layers and datasets considered to have long-term or continuing informational or historical value to ensure proper retention of this data. See also “GEOGRAPHIC INFORMATION SYSTEMS (GIS) SOURCE DOCUMENTS/DATA,” “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.

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.

Electronic Communications as Public Records

Electronic communication is the electronic transfer of information, typically in the form of electronic messages, memoranda, and attached documents, from a sending party to one or more receiving parties by means of an intermediate telecommunications system. Electronic communications include e-mail, instant messaging, text messaging (such as SMS, Blackberry 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. Electronic communications created or received in connection with the transaction of official business are public records subject to inspection and copying in accordance with Chapter 119, Florida Statutes, and subject to applicable state retention laws and regulations, unless expressly exempted by law.

Electronic communications created or received for personal use are not generally considered public record and do not fall within the definition of public records simply by virtue of their placement on a government-owned computer system. However, if an agency discovers misuse of their electronic communications system and personal electronic messages are identified as being in violation of the agency's policy, the electronic messages may become public record as part of an investigation.

Retention Requirements for Electronic Communications

All public records must have an approved retention schedule in place before they can be destroyed or otherwise disposed of. As indicated above under **Retention Requirements for Electronic Records** (page 11), retention periods are determined by the content, nature, and purpose of records, and are set based on the legal, fiscal, administrative and historical values, regardless of physical 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. Therefore, there is no single retention schedule that applies to all electronic messages or communications. The retention period 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 record 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" record series. "Transitory" refers to short-term ***value*** based upon the content and purpose of the message, ***not*** the format or technology used to transmit it. Examples of transitory messages include, but are not limited to, e-mail messages or other communications reminding employees about scheduled meetings or appointments; most telephone messages (whether in paper, voice mail, or other electronic form); announcements of office events such as holiday parties or group lunches; and recipient copies of announcements of agency-sponsored events such as exhibits, lectures, workshops, etc.

Transitory messages are not intended to formalize or perpetuate knowledge and do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt. The retention requirement for transitory messages is "retain until obsolete, superseded or administrative value is lost." Therefore, electronic communications that fall into this category can be disposed of at any time once they are no longer needed.

Agencies that allow the use of electronic communications on their networks, including e-mail, instant messaging, text messaging (such as SMS, Blackberry 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 must recognize that such content may be a public record and must manage the records accordingly. The seemingly ephemeral nature of some electronic communications heightens the need for users to be aware that they may be creating public records using these technologies and must properly manage and preserve record content. Agencies must make sure the systems in use allow them to adhere to all retention requirements.

Agencies developing a comprehensive policy need to ensure that electronic communications content is managed consistently across the agency in its component offices. An effective policy addresses the authorized use of the various electronic communications technologies and provides guidelines for the management of the records generated by these communications. This is especially important because electronic communications content may be subject to various types of access requests, including public records requests or as part of a discovery process in a litigation context.

Sorting electronic communications such as e-mail into appropriate personal folders is a helpful way to manage these records and to ensure that appropriate retention requirements are identified and met. That is, just as file cabinets are set up to house different sets of files, and employees know where to file paper records in those files, e-mail files and folders can be set up with the appropriate retention period designated for each of those files and folders. If no retention schedule exists for records relating to a particular activity, then one must be established and that retention schedule would then apply to all documentation of that activity, regardless of format (paper, microfilm, electronic, etc.).

E-mail Archiving

Although e-mail archiving applications may provide business benefits to an agency, e-mail archiving applications can be limited in their capabilities to keep and organize records according to records management laws, regulations, and policies. If an agency decides to use e-mail archiving applications to manage public records, the agency must ensure that records management requirements are addressed.

E-mail archiving generally refers to applications that remove e-mail from the mail server and store it in a central location also known as an archive. IT professionals use the term "archiving" to mean the copying or transfer of files for storage. In general, these applications collect in a central archives or “repository” the e-mail (which may include attachments, calendars, task lists, etc.) of some or all agency users. E-mail archiving

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:

- Current e-mail archiving applications may not be capable of grouping related records in accordance with recordkeeping requirements or maintaining the records in a usable format for their full required retention periods;

- It may make it difficult to identify and distinguish between permanent records and short-term records and carry out proper disposition at the end of their retention periods, be that destruction of records or transfer to the State Archives of Florida or a local historical records repository;

- An agency that adopts e-mail archiving while continuing a print and file policy for official e-mail records could unintentionally undermine records management compliance as users may assume that the e-mail application has replaced the e-mail print and file policy; therefore, an agency should provide clear guidance if print and file should be done in addition to e-mail archiving.

If an e-mail archiving application is adopted as the only means of storing e-mail messages, agencies must use e-mail archiving technologies in conjunction with additional controls such as records management policies and procedures, business rules, and other conditions necessary to ensure compliance with records management requirements. Any agency that adopts e-mail archiving applications as its means of official recordkeeping must create policies, provide adequate user training, and take steps to identify and manage the limitations in current e-mail archiving applications in order to ensure that records are kept according to public records laws and rules.

E-Discovery

Electronic discovery (or e-discovery) refers to discovery in civil litigation of electronically stored information, or ESI. The widespread use of computers to conduct business in both the private and public sectors, as well as for personal use, has forced the courts to address the unique challenges posed by using ESI as evidence in the legal process. As a result, the Federal Rules of Civil Procedure (FRCP) were amended in December 2006 to address e-discovery.

The FRCP amendments do not require agencies to keep all of their e-mails (or other electronic records) permanently. In fact, these amendments do not address records retention periods at all. However, they do underscore the importance of applying records management policies, practices, and procedures to electronic records, and the value of having electronic records policies in place that explicitly accommodate records management requirements.

Further, recent case law demonstrates that courts expect organizations to produce ESI in the same electronic format in which the organization normally created or maintained it for business purposes. Therefore, in the event of litigation or reasonably anticipated litigation, existing records in electronic form must be maintained in their current electronic format; printing them out or converting them to another format at that point might not only be unnecessary, but also might be unacceptable to the court. If an agency has a print and file policy for e-mail, deletion of e-mails once printed must be suspended until all legal discovery issues are closed.[6]

Agencies that are already following State of Florida records management requirements and guidelines and working with their legal office to ensure that records relating to litigation are retained as long as required for that litigation are already doing most of the things necessary to accommodate the FRCP e-discovery amendments. Agencies can do the following to prepare for e-discovery:

- Have a formal, active records management program and policy which applies to all records regardless of format.
- Maintain records inventories or other means of identifying and locating all agency records.
- Ensure that retention schedules and all other retention requirements have been met before disposing of records in any form, including electronic records.

[6] See, for example, *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Secs,* No. CIV. 05-9016, 2010 U.S. Dist. LEXIS 1839 (S.D.N.Y. Jan. 11, 2010) and subsequent amended opinions; *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212 (S.D.N.Y. 2003); and *Vagenos v. LDG Fin. Servs., LLC,* No. 09-cv-2672, 2009 WL 5219021 (E.D.N.Y. Dec. 31, 2009).

- Properly document disposition of records.
- Have a formal procedure for placing a litigation hold on records in all formats that might be relevant to anticipated, pending, or ongoing litigation.
- Ensure regular consultation among agency legal staff, RM, and IT staff.

Consultation between agency legal staff, records management staff, and information technology staff is critical to ensuring that all the pieces are in place and all the key players are familiar with their responsibilities relating to e-discovery and other records management requirements. Agencies should consult with their legal counsel to verify their legal requirements for compliance with these and other rules of civil and criminal procedure.

The complete text of the FRCP e-discovery amendments and the accompanying committee notes (commentary) by the Advisory Committee on the Rules of Civil Procedure are available on the United States Courts website in pdf format at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/EDiscovery_w_Notes.pdf. A few key provisions of interest to records managers are briefly summarized below. The following summary is not intended to be, and should not be construed to be legal advice. For more information on the legal obligations that these and other provisions impose, agencies should refer to the full text and consult their legal counsel.

Pretrial Conferences: The judge's pretrial conference scheduling order may include "provisions for disclosure or discovery of electronically stored information" [FRCP Rule 16(b)(5)]. According to the Committee Note, this amendment is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation.

Required Disclosures: Each party (an individual or organization involved in a legal proceeding) must, "without awaiting a discovery request, provide to other parties . . . a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment" [FRCP Rule 26(a)(1)(B)]. According to the Committee Note, this amendment clarifies "that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses."

Undue Burden: A party is not required to provide discovery of electronically stored information if that information is "not reasonably accessible because of undue burden or cost." The party must be able to demonstrate that undue burden or cost, but the court may still order discovery upon showing of good cause by the requesting party [FRCP Rule 26(b)(2)(B)]. According to the Committee Note, "The responding party has the burden [to show that] the identified sources are not reasonably accessible in light of the burdens

and costs [and] the requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information."

Discovery Planning Conferences: Prior to a scheduling conference or scheduling order, parties must discuss issues and develop a discovery plan, including "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced" [FRCP Rule 26(f)(3)]. According to the Committee Note, this amendment directs parties "to discuss discovery of electronically stored information during their discovery-planning conference" if electronic discovery is anticipated.

Option to Produce Records in Response to Interrogatories: A party served with an interrogatory that can be answered from an examination of that party's records, including electronically stored information, may "specify the records from which the answer may be derived or ascertained and [allow] the party serving the interrogatory . . . to examine, audit or inspect such records and to make copies, compilations, abstracts, or summaries" [FRCP Rule 33(d)]. According to the Committee Note, the "responding party [may] substitute access to documents or electronically stored information" under specified circumstances.

Production of Electronically Stored Information: A party may request another party to produce "any designated documents or electronically stored information . . . The request may specify the form or forms in which electronically stored information is to be produced . . . if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or . . . reasonably usable . . . a party need not produce the same electronically stored information in more than one form" [FRCP Rule 34(a, b)]. According to the Committee Note, this amendment "confirm[s] that discovery of electronically stored information stands on equal footing with discovery of paper documents." Rule 34(b) "protect[s] against . . . production in ways that raise unnecessary obstacles for the requesting party."

Failure to Make Disclosure or Cooperate in Discovery: This amendment, known as the "safe harbor" provision, prohibits sanctions under this rule, "[a]bsent exceptional circumstances," for "failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system" [FRCP Rule 37(f)]. According to the Committee Note, this amendment recognizes that "the routine alteration and deletion of information . . . attends ordinary use" of computers. "The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve."

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 expenditure on hardware and software. Services may include data storage and management, software, and computing resources. This service delivery model is attractive for its "potential cost savings brought about by economies of scale and the ability to rapidly deploy new applications and services. Cloud computing has the potential to have a substantial impact on archival and records management programs as well."[7]

Agencies thinking of using cloud computing should make sure they have a clear understanding of exactly what is being proposed. Records management requirements will apply to public records maintained in the cloud just as they would if the records were stored on agency computers. Some of the issues that should be considered are listed below.

Scope – What agency records will be stored, processed, or accessed through the cloud? Will they include confidential or exempt records?

Retention – With cloud computing services, often multiple copies of the data are stored on geographically-dispersed resources for data protection and access. How will the vendor ensure destruction of all copies of records that have met their retention?

Location – It is not uncommon for the end-user to have no idea where their information is stored or processed in the cloud. If agency records must be maintained within jurisdictional boundaries, this requirement should be included in the vendor contract.

Legal/Policy Compliance – Cloud computing may not adequately address some compliance issues such as those related to the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act of 2002, and the Payment Card Industry (PCI) security requirements.

E-Discovery – How will the agency ensure that it can comply with an e-discovery order if some or all of its records are stored in the cloud?

Interoperability – As with any information technology, it is important to ensure that records are not trapped in a proprietary system in the cloud that will require considerable expense or effort to remove it from that system or move it to another system.

[7] Conrad, Mark, "Distributed Computing – Cloud Computing and Other Buzzwords: Implications for Archivists and Records Managers." *Crossroads* 2009, no. 3. CERIS White Papers. http://www.nagara.org/associations/5924/files/Crossroads_2009_3.pdf

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 records laws and rules.

Rule 1B-26.003, *Florida Administrative Code*, states that "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." Agencies should study the pros and cons of automation rather than assuming automation is the best choice. For example, conversion of paper records to electronic format is not always the best option for maintaining records, particularly records that only have to be retained for a short period of time. The cost of converting short-term records may be greater than simply storing the records in paper format until they are eligible for disposal. If the agency has a high volume of short-term records, off-site storage can be an economical alternative to keeping the records in the office or scanning them.

Incorporate Recordkeeping Requirements into System Design

Rule 1B-26.003, *Florida Administrative Code*, further states that "recordkeeping requirements must be incorporated in the system design and implementation of new systems and enhancements to existing systems." Agencies must "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." Recordkeeping requirements are best addressed and incorporated when automated systems are being planned and designed. Selected technologies must accommodate records retention, exemption, and access requirements. For instance, an agency implementing a new surveillance recording system must ensure that the system is capable of accommodating the minimum 30-day retention requirement for surveillance recordings as well as the ability to preserve the recordings longer in the event of an incident investigation (*General Records Schedule GS1-SL for State and Local Government Agencies*, Item #302, Surveillance Recordings).

If an agency utilizes an information system development methodology (ISDM), system development life cycle (SDLC), or similar process when designing and planning information systems, records management requirements should be included in the earliest stages of this process.

Agencies should include steps to ensure that:

- All records are covered by records retention schedules approved by the Division of Library and Information Services.
- Records can be migrated to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.
- Provisions are made for providing access to records which are not exempt from disclosure.
- Records can be disposed of when they have met their required retention. Disposal might be destruction of records or transfer to the State Archives of Florida or a local historic records repository for permanent preservation. Destruction of public records must be in accordance with Rule 1B-24.003(10), *Florida Administrative Code*.
- Records needed for legal discovery are withheld from disposal and retained in their native format until litigation is resolved.

These recordkeeping requirements should be incorporated into the agency's procedures and apply when the agency contracts with any person or entity for services as well as when systems are developed in house.

Document Electronic Recordkeeping Systems

Maintaining documentation of all agency systems that store electronic records is a best practice for both records management and information technology; often, but not always, the IT program maintains such documentation. Documentation does not necessarily have to be completely separate for each and every application, as long as it is sufficient to ensure preservation and access to all of the records for as long as they need to be maintained by the agency.

Agency RM and IT staff should work together to ensure the development of up-to-date documentation for all agency electronic records systems that is adequate to specify all technical characteristics necessary for reading or processing the records and the timely, authorized disposition of records. Documentation includes written descriptions and procedures that provide information about a computer program or a computer system so that it can be properly used and maintained. The documentation should also:

- Identify all defined inputs and outputs of the system,
- Define the contents of the files and records,
- Determine restrictions on access and use,
- Provide an understanding of the purpose(s) and function(s) of the system, and

- Describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information.

For purchased software, the documentation supplied by the software vendor, along with any agency-specific documentation that IT maintains such as user permissions, etc., should be sufficient. The agency should develop similar documentation for software that is developed in-house.

Agencies must establish and adopt procedures for external labeling of the contents of diskettes, disks, tapes, and optical disks so that all authorized users can identify and retrieve the stored information.

Refer to Rule 1B-26.003(7), *Florida Administrative Code*, for other specific documentation standards and requirements. Regardless of how an agency's electronic records are stored, subsection (7) of the rule is intended to ensure that all of the records can be identified, accessed, and read.

Provide Training for Users of Electronic Records

Agencies must provide for users of the systems to be trained in the operation, care, and handling of the equipment, software, media used in the system, and system security controls.

Training for individuals who create, edit, store, retrieve, or dispose of records is an important aspect of electronic records management. Training should enable agency personnel to identify public records, understand how records are filed in an electronic recordkeeping system, how records are safeguarded, what procedures are used to edit records, and how records should be disposed of according to legal requirements.

Agencies must 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.

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

- Classroom training, offered several times a year on a recurring basis or as needed for special situations.

- A self-learning center within the agency, where operators can teach themselves at their own rates of learning through interactive programs. The commercial tutorial programs do not usually include records management information, but tutorials teaching records management concepts for electronic records could be developed by the agency.

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

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

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.

Section 92.29, Florida Statutes, provides that "photographic reproductions or reproductions through electronic recordkeeping systems…shall in all cases and in all courts and places be admitted and received as evidence with a like force and effect as the original would be…" To enhance the legal admissibility of electronic records, Rule 1B-26.003, *Florida Administrative Code*, requires that agencies:

- Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.
- Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure systems are protected against such problems as power interruptions.
- 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.

Sustainable Formats

Typically, agencies select electronic formats based on business needs and current technical requirements. Selected formats must be sustainable, that is accessible both throughout their lifecycle and as technology evolves, regardless of the technology used when it was originally created. A sustainable format is one that increases the likelihood of a record being accessible in the future. Formats that are not sustainable may cause records to become obsolete and inaccessible before they are eligible for deletion as authorized in the approved records retention schedule.

Rule 1B-26.003, *Florida Administrative Code*, defines long-term records as those with a retention requirement of more than 10 years. When records need to be maintained over the long term (sustainability), agencies should consider each of the following characteristics of formats:

- **Published Documentation and Open Disclosure** - Publicly and openly documented formats adhere to specifications that are published and accessible. Publicly accessible specifications allow developers to create a wide variety of applications to read, process, and validate files. Openly documented specifications assist developers in creating tools to access the information in obsolete formats, and/or assist in migrating files to future formats. Tagged Image

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

policies and procedures governing creation and management of electronic records and adhere to approved records retention schedules to further ensure that records are maintained properly.

Selecting Storage Media

As specified in Rule 1B-26.003(10), *Florida Administrative Code*, agencies must select appropriate media for storing record (master) copies of electronic public records throughout their life cycle that meet the following requirements:

- Permit easy and accurate retrieval in a timely fashion;
- Retain the records in a usable format until their authorized disposition; and
- When appropriate, meet the requirements necessary for transfer to the State Archives of Florida.

Agencies should consider the following factors before selecting a storage media or converting from one media to another:

- The authorized retention of the records;
- The maintenance necessary to retain the records;
- The cost of storing and retrieving the records;
- The access time to retrieve the stored records;
- The portability of the medium (can be read by multiple manufacturer's equipment);
- The ability to transfer the information from one medium to another.

When storing permanent or long-term records, agencies must adhere to additional standards. Long-term records are defined as those that have an established retention of more than 10 years.

- Agencies shall not use floppy disks, audio cassettes, or VHS-format video cassettes for the storage of record (master) copies of permanent or long-term records.
- Permanent or long-term records on magnetic tape shall be stored on polyester-based media.
- Agencies shall use only previously unrecorded audio or video tape for record (master) copies of permanent or long-term audio or video recordings.

- 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 expectancies are often cited as 10 years, 25 years, or longer. A variety of factors discussed in the source references below (page 33) may result in a much shorter life span for CDs/DVDs. Life expectancies are statistically based; any specific medium may experience a critical failure before its life expectancy is reached. Additionally, the quality of your storage environment may increase or decrease the life expectancy of the media. We recommend testing your media at least every two years to assure your records are still readable.

Agencies should develop policies and procedures to ensure access to electronic records stored for a long duration on CDs or DVDs. Some things you should consider as you develop your policies and procedures are:

- The disk should be read immediately after writing and/or before storing it to verify that what was written is what was intended, that it is readable, and that it conforms to your inventory.

- Disks might only be readable on the specific drive on which they were originally recorded or on some other compatible drive.

- The data recorded onto CDs/DVDs should not be "zipped."

A detailed inventory of the content of each CD/DVD should be created and maintained. This includes information sufficient to locate an individual record, including identifiers that maintain the uniqueness of the record within the collection. To ensure the records contained on the CD/DVD can be retrieved and/or migrated when necessary, include the name and version of the software application for each file (e.g., Microsoft Word 2007) on your detailed inventory.

Disks should be handled only by the outer edge or the center hole, never by touching the surface. Fingerprints can disrupt the tracking of the laser on the disk. Follow the manufacturer's instructions to remove any dirt, fingerprints, or smudges.

[10] http://www.osta.org/technology/cdqa13.htm.

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) (http://www.uni-muenster.de/Forum-Bestandserhaltung/downloads/iraci.pdf).

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.

- Ease of administration. The policy should work with your computer infrastructure, so that you can monitor policy compliance, manage records and records series, gather metadata (metadata in the context of records management is data describing context, content, and structure of records and their management through time), and perform other administrative tasks easily and in compliance with all legal requirements. For example, if all the records in a specific record series are easily identifiable by file name, they will be easier to gather and manage.

- Uniqueness. To avoid file names conflicting when they are moved from one location to another, each record's file name should be unique. Having multiple files with the same name is confusing and there is the danger that a file might automatically overwrite another file with the same name. How you arrive at unique file names will require some thought. Once you have developed a system, it is important to standardize and adhere to it.

- Version control. Determine how and whether to indicate the version of the record. Sometimes current and obsolete drafts are put in different electronic file folders without altering the file name. However, when these records are moved from the active electronic file folder to another storage area, identical file names may conflict and cause confusion.

- Scalability. Consider how scalable your file naming policy needs to be. For example, if you want to include the project number, don't limit your project numbers to two digits, or you can only have ninety-nine projects.

- Persistence over time. File names should outlast the records creator who originally named the file. With good staff input, and training, you should be able to develop file names that make sense to staff members once the file creators are no longer available.

Automated Systems to Manage Electronic Records

Agencies may want to consider acquiring computer software written specifically to manage electronic records. These systems can be costly and require a substantial commitment to implement, but they offer features that help control documents and records and some have built in records management features to help safeguard the agency’s records. Agencies considering acquiring such systems should understand the differences in the types of system available.

Electronic Records Management Systems (ERMS) are designed primarily to manage an organization’s electronic records, although they can be used for some physical records management functions also. ERMS functionality includes capture of electronic records and their accompanying metadata, discovery, records retention in accordance with set schedules or rules, authorized disposition, litigation holds, and other functionality designed to ensure the appropriate maintenance, accessibility, authenticity, and security of records for as long as required by the organization.

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 storage structure, which may be under the control of users; • is intended primarily to support day-to-day use of documents for ongoing business.	• prevents records from being modified; • prevents records from being deleted except in certain strictly controlled circumstances; • must include rigorous retention controls; • must include a rigorous record arrangement structure (classification scheme) which is maintained by an administrator; • may support day-to-day working, but is also intended to provide a secure repository for business records.

The United States Department of Defense (DoD) has developed functional requirements and standards for that Department's electronic records management systems which can be helpful to Florida agencies planning to acquire these types of systems. DoD standard DoD 5015.2-STD, Electronic Records Management Software Applications Design Criteria Standard, April 25, 2007, is a requirement for DoD records management applications and is endorsed by the National Archives for use by all federal agencies. The federal government certifies compliant software as meeting the requirements of the DoD standard and provides a list of certified products. The standard is available at http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf and the register of compliant software applications is available at http://jitc.fhu.disa.mil/recmgt/register.html. While not a requirement for Florida agencies, the DoD standard can serve as a useful reference for evaluating ERMS software and a basis upon which agencies can develop their own functional requirements.

Another useful resource is the European Commission's Model Requirements for the Management of Electronic Records (MoReq2). This publication is a model set of requirements that users can adapt to their needs when developing or selecting systems for

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.

Frequently Asked Questions (FAQ)

1. What are the requirements for scanning public records?

Public records must be scanned in accordance with Rule 1B-26.003, *Florida Administrative Code*. For records with a minimum retention of over 10 years, the rule states that the records must be scanned at a minimum 300 dpi and use "a published International Organization for Standardization (ISO) open standard image format." These formats include TIFF, PDF, PDF/A, and others. To find out if a particular format is ISO-approved, go to the ISO website at http://www.iso.org/ and search for the format (e.g., search for PDF, TIFF, etc.).

For records with a minimum retention requirement of 10 years or less, any dpi and image format can be used; however, the agency still must ensure that the records remain accessible and readable for as long as they are required to be retained.

2. If I scan my records, can I get rid of the original hard copy?

In general, scanned images of public records can be designated as the record (master) copies of the records, and the original hard copy can be designated as duplicates and disposed of when no longer needed, provided that the electronic records are in compliance with Rule 1B-26.003, *Florida Administrative Code*, and the completeness and accuracy of the scanned copies have been verified. The electronic version can then be designated the record (master) copy and as such must be retained for the length stated in the applicable retention schedule and in accordance with Rule 1B-26.003, *Florida Administrative Code*. The paper original can then be designated as a duplicate and disposed of at any time.

However, Rule 1B-24.003(9)(a), *Florida Administrative Code*, states "… An agency that designates an electronic or microfilmed copy as the record (master) copy may then designate the paper original as a duplicate and dispose of it in accordance with the retention requirement for duplicates in the applicable retention schedule unless another law, rule, or ordinance specifically requires its retention." Although this is a rare exception, we recommend that agencies consult with their legal counsel for guidance if they are unsure if their records have to be maintained in paper form.

3. How long do we have to keep our e-mail?

Retention of e-mail and other electronic communications, as with retention of records in any other format, is based on the *content* of the particular e-mail or electronic message. As stated in the *General Records Schedule GS1-SL for State and Local Government Agencies*:

ELECTRONIC COMMUNICATIONS
There is no single retention period that applies to all electronic messages or communications, whether they are sent by e-mail, instant messaging, text messaging (such as SMS, Blackberry

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 **E-Discovery** section (page 18), in the event of litigation or reasonably anticipated litigation, existing records in electronic form must be maintained in their current electronic format until all legal discovery issues are closed.

5. How long do we have to keep our back-ups? Should we keep e-mail back-ups permanently in case they are ever needed?

As stated in the *General Records Schedule GS1-SL for State and Local Government Agencies:*

BACKUP TAPES
There is no retention schedule for back-up tapes or other forms of data back-up. A back-up tape or drive should be just that: a data/records back-up kept solely as a security precaution but not intended to serve as the record copy or as a records retention tool. In the case of disaster, the back-up would be used to restore lost records; otherwise, 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 your

server) the only existing copy of an item that has not met its retention period is on a back-up tape or drive, the custodial agency of that record 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.

6. Are postings or messages on our website, Facebook page, or Twitter site public records? If so, how long do we have to keep them?

If postings on a website or social networking site meet the definition of a public record, then they would, indeed, be public records. The retention of the postings will be determined by the content, nature, and purpose of the posting. Just like e-mail and other forms of electronic communication, no single retention period would necessarily apply to all of the postings.

Attorney General's Opinion Number AGO 2009-19 (April 23, 2009) states the following regarding Facebook pages established by a city – this will of course apply to any public agency maintaining a Facebook page:

> Since the city is authorized to exercise powers for a municipal purpose, the creation of a Facebook page must be for a municipal, not private purpose. The placement of material on the city's page would presumably be in furtherance of such purpose and in connection with the transaction of official business and thus subject to the provisions of Chapter 119, Florida Statutes. In any given instance, however, the determination would have to be made based upon the definition of "public record" contained in section 119.11, Florida Statutes. . .
>
> The city is under an obligation to follow the public records retention schedules established by law. . .
>
> Communications on the city's Facebook page regarding city business by city commissioners may be subject to Florida's Government in the Sunshine Law, section 286.011, Florida Statutes. Thus, members of a city board or commission must not engage on the city's Facebook page in an exchange or discussion of matters that foreseeably will come before the board or commission for official action. . .
>
> It is the nature of the record created rather than the means by which it is created which determines whether it is a public record.[5] The placement of information on the city's Facebook page would appear to communicate knowledge. Thus, the determination in any given instance as to whether information constitutes a public record will depend on whether such information was made or received in connection with the transaction of official business by the city. . .

Similarly, a 2009 Department of State's General Counsel's Office opinion states that "A posting or comment to a state agency page on a social networking site is a public record

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.

So it is the nature, content, and purpose of the record that will determine if it meets the definition of public record and, if so, what the retention of that record would be. While some Twitter messages ("tweets") might indeed be transitory messages, other "tweets" might fall under other retention schedules, such as one of the CORRESPONDENCE items, again depending on the content of the message. Just as with public records in any other form, agencies will need to determine the appropriate retention item based on the nature, content, and purpose of the record and ensure that it is retained for that period of time.

One possible option when using Facebook or some other social networking technologies is to disallow postings from outside sources, thus saving the agency the trouble of determining and implementing retention requirements for those outside postings. If outside postings are allowed, the agency will need to find a way to ensure the appropriate retention of those postings that are public records. **We advise agencies to carefully consider public records access and retention requirements, responsibilities, and implications when considering the use of any social networking technologies.**

7. What are Florida's requirements for electronic signatures?

The statutory governance for electronic signatures is Florida's Electronic Signature Act of 1996, Section 668.001-006, Florida Statutes, and Uniform Electronic Transaction Act, Section 668.50, Florida Statutes. In particular, the following sections may apply:

> 668.004 Force and effect of electronic signature.--Unless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature.
>
> 668.50(7) LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.—
>
> (a) A record or signature may not be denied legal effect or enforceability solely because the record or signature is in electronic form.
>
> (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in the formation of the contract.

> (c) If a provision of law requires a record to be in writing, an electronic record satisfies such provision.
>
> (d) If a provision of law requires a signature, an electronic signature satisfies such provision.
>
> 668.50(13) ADMISSIBILITY IN EVIDENCE.--In a proceeding, evidence of a record or signature may not be excluded solely because the record or signature is in electronic form.

In essence, unless otherwise specified by law or administrative rule, digital signatures are acceptable. Agencies are advised to review Chapter 668, Florida Statutes, as well as consult with their legal counsel for further guidance on this issue.

APPENDIX A - Department of State E-Mail Policy

Florida Department of State
Policies and Procedures

ELECTRONIC MAIL POLICY

1. Scope

This policy provides guidelines for the management and usage of electronic mail (e-mail) messages as public records within the Florida Department of State ("Department"). This policy applies to the entire Department workforce with access to the Department's e-mail system including all offices, divisions, bureaus, advisory bodies, and contract agents of the Department in the conduct of their official duties as prescribed by law.

This policy does not provide specific procedures for system backups or "archiving" of inactive e-mail. Employees should refer to internal Department operating procedures for this information.

2. Purposes

The purposes of this policy are to:

a. Ensure that Department employees comply with Florida's Public Records Law, Chapter 119, Florida Statutes, when using the Department's e-mail system;

b. Ensure that Department employees properly manage and retain e-mail as public records in accordance with applicable records management statutes and rules; and

c. Ensure proper usage of the Department's e-mail system and that users understand the types of e-mail usage that are considered inappropriate and a violation of this policy.

3. Authority

a. Chapters 119, 257, and 282, Florida Statutes;

b. Rules 1B-24 and 60DD-2, Florida Administrative Code.

4. Definition of E-Mail

E-mail is the electronic transfer of information, typically in the form of electronic messages, memoranda, and attached documents, from a sending party to one or more receiving parties by means of an intermediate telecommunications system.

5. E-Mail as a Public Record

a. E-mail which is created or received by a Department employee in connection with the transaction of official business of the Department is considered a public record and is subject to inspection and/or copying in accordance with Chapter 119, Florida Statutes, and is subject to applicable state retention laws and regulations, unless expressly exempted by law.

b. E-mails created or received for personal use are not generally considered public records and do not fall within the definition of public records by virtue of their placement on a

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,*

intimidating, defamatory, derogatory, violent or which contains profanity or vulgarity, regardless of intent. Among those which are considered offensive include, but are not limited to, messages containing jokes, slurs, epithets, pictures, caricatures, or other material demonstrating animosity, hatred, disdain or contempt for a person or group of people because of race, color, age, national origin, gender, religious or political beliefs, marital status, disability, sexual orientation or any other classification protected by law.

h. Sending messages or requesting information reflecting or containing chain letters or any illegal activity, including, but not limited to gambling.

i. Sending or requesting information or material that proselytizes or promotes a religious or political view, cause, position or action.

8. No Right of Privacy

Department employees have no right of personal privacy in any material created, stored in, received, or sent over the Department's e-mail system. The Department reserves and may exercise the right, at any time and without prior notice or permission, to intercept, monitor, access, search, retrieve, record, copy, inspect, review, block, delete and/or disclose any material created, stored in, received, or sent over the Department's e-mail system for the purpose of protecting the system from unauthorized or improper use or criminal activity.

9. Retention Requirements for E-Mail

a. All public records must have an approved retention schedule in place before they can be destroyed or otherwise disposed of. 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 their form. Therefore, there is no single retention schedule that would apply across the board to all e-mails. E-mail, like other records, irrespective of its form, can have a variety of purposes and relate to a variety of program functions and activities. The retention period of any particular e-mail message will generally be the same as the retention for records in any other form that document the same program function or activity.

b. Department employees are required to relate each e-mail that is created or received by the employee through the Department's e-mail system to the activity it documents, as well as to other records documenting that activity, and apply the appropriate retention period based on that activity or function. Approved retention schedules for State Government Agencies can be found at http://dlis.dos.state.fl.us/recordsmgmt/gen_records_schedules.cfm

c. It is the responsibility of each Department employee to ensure that e-mail and other public records in their custody are maintained for the required retention period(s). Although the Department routinely backs up its servers, each back-up is maintained only briefly for disaster recovery purposes and therefore cannot be regarded as a tool for meeting public records retention requirements.

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. For instance, an e-mail message notifying employees of an upcoming meeting would only have value until the meeting has been attended or the employee receiving the message has marked the date and time in the calendar. The informal nature of transitory messages might be compared to a telephone conversation or a conversation in an office hallway. The retention requirements for Transitory Messages is "Retain until obsolete, superseded or administrative value is lost." Therefore, e-mails that fall into this category can be disposed of at any time once they are no longer needed.

11. Managing E-mail

Sorting e-mail into appropriate personal folders is a helpful way to manage these records and to ensure that appropriate retention requirements are identified and met. That is, just as file cabinets are set up to house different sets of files and employees know where to file paper records in those files, e-mail files and folders can be set up with the appropriate retention period designated for each of those files and folders. If no retention schedule exists for records relating to a particular activity, then one must be established and that retention schedule would then apply to all documentation of that activity, regardless of form (paper, film, electronic, etc.).

12. Violations

Violations of this policy may result in disciplinary action, up to and including termination of employment.

APPROVED BY:

Original Signature on File

_____

Dawn Roberts
Assistant Secretary of State/Chief of Staff

Date Approved: 4/18/07

This policy amends the Department's E-Mail Policy dated June 30, 2005, to update references to the General Records Schedule in Section 10.

APPENDIX B - Records Inventory Worksheet

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

RECORDS INVENTORY WORKSHEET

Department/ Section	Contact	Phone No.

Location of Records Room File	Schedule No.	Item No.

Records Series Title

Record/File Title

Description (Contents, Purpose, and Use: Include form title and numbers, if any)

☐ Record Copy ☐ Duplicate Copy

File Type	Cut-Off Date	Arrangement	Authorization for Series
☐ Subject ☐ Case/Business Activity ☐ Working Papers ☐ Reference ☐ Index	☐ Calendar Year ☐ Fiscal Year ☐ Anniversary ☐ Continuous ☐ Other _____	☐ Alphabetic by _____ ☐ Alphanumeric by _____ ☐ Numeric by _____ ☐ Chronological by _____ ☐ Other _____	☐ a. Statute ☐ b. Regulations ☐ c. Administrative _____ (Citation)

Record Form

☐ 8-1/2" x 11" paper (letter size)	☐ 11" x 15" computer printouts	☐ Computer disks
☐ 8-1/2" x 14" paper (legal size)	☐ 11" x 8-1/2" computer printouts	☐ Compact discs
☐ Bound books, catalogs	☐ Roll microfilm	☐ Computer tapes/cartridges
☐ 3" x 5" Cards	☐ Microfiche	☐ Video tapes
☐ 4" x 6" Cards	☐ Other _____	☐ Optical discs

Electronic Records Filing

a. What is the name of the system?
b. Who owns the system?
c. What operating system is needed to retrieve and view files?
d. What application software is needed to retrieve and view files?
e. What is the file format? (.doc, .xls, .tif, .rtf, etc.)
f. What is current age of media on which records are stored? (1 year, 5 years, etc.)
g. How quickly is this information usually needed? (within minutes, days, weeks, etc.)
h. How often is this information accessed? (daily, weekly, monthly, etc.)
i. What business activity do these records support?
j. Are there any records related to these records?
k. Do you need more assistance with assessing these records?

Current Holdings

Year (Inclusive Dates)	Paper Cubic Feet	Electronic Bytes/Item Count	Type Filing Equipment Used	Quantity

How active are these records?	Who uses these records?
☐ Active (accessed frequently; weekly or immediately) ☐ Semi-active (accessed periodically; monthly or less often) ☐ Inactive (no need to retain in the active office area)	

Place an "X" in the proper column (If the answer is "yes", please explain below.)	YES	NO
1. Is this Department the official record holder?	☐	☐
2. Are there copies of this record series (or major portion of it) in this Department?	☐	☐
3. Are there copies of this record series (or major portion of it) in another Department?	☐	☐
4. Does this record series contain information exempt from public access?	☐	☐
5. Is there any legal requirement affecting disposal of this record series?	☐	☐
6. Does this record series contain information subject to regulatory requirements?	☐	☐
7. Does this record series contain information subject to legal requirements?	☐	☐
8. Does this record series contain information used in or subject to audits?	☐	☐
9. Is this record series needed because of archival or historic interest?	☐	☐
10. Are these vital records?	☐	☐

Responses to Questions and Additional Comments

Retention		Recommended Retention	
Inventoried By	Date	Reviewed By	Date

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:
(a) “ASCII” means the American Standard Code for Information Interchange, a 7-bit coded character set for information interchange which was formerly ANSI (American National Standards Institute) Standard X3.4 and has since been incorporated into the Unicode standard as the first 128 Unicode characters.
(b) “Database” means an organized collection of automated information.
(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. It also controls the security and integrity of the database.
(d) “Digital signature” means a type of electronic signature (any letters, characters, or symbols executed with an intent to authenticate) that can be used to authenticate the identity of the sender of a message or the signer of a document and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures can be created through hashing algorithms.
(e) “Electronic record” means any information that is recorded in machine readable form.
(f) “Electronic recordkeeping system” means an automated information system for the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures.
(g)“Hashing algorithm” (hash function, checksum) means a formula or procedure for checking that electronically transmitted messages or documents have not been altered by transforming a string of characters into a usually shorter fixed-length “hash value” or key that represents the original string. The receiver of the message can execute the same hashing algorithm as the sender and compare the resulting hash values; any difference in the hash values indicates an alteration of the message or document sent. Hashing algorithms can be used to create digital signatures.
(h) “System design” means the design of the nature and content of input, files, procedures, and output and their interrelationships.
(i) “Permanent or long-term records” means any public records as defined by Section 119.011(11), F.S. which have an established retention period of more than 10 years.

(j) “Record (master) copy” means public records specifically designated by the custodian as the official record.
(k) “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.
(l) “Open format” means a data format that is defined in complete detail, allows transformation of the data to other formats without loss of information, and is open and available to the public free of legal restrictions on use. An open format may be either standards-based or proprietary. (m) “Unicode” means the universal character encoding standard maintained by the Unicode Consortium, providing the basis for processing, storage, and interchange of text data in any language in all modern software and information technology protocols.

(6) AGENCY DUTIES AND RESPONSIBILITIES. Each agency shall:
(a) Develop and implement a program for the management of electronic records.
(b) Ensure that all records are included within records retention schedules, either by being included within an applicable General Records Schedule, or by developing and obtaining approval for an individual agency-specific records retention schedule in accordance with Rule 1B-24.003, F.A.C., Records Retention Scheduling and Dispositioning.
(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 recordkeeping systems in the operation, care, and handling of the equipment, software, and media used in the system.
(g) Ensure that agency electronic recordkeeping systems meet state requirements for public access to records in accordance with Chapter 119, F. S.
1. STANDARD. Each agency which maintains public records in an electronic recordkeeping system shall provide, to any person making a public records request pursuant to Chapter 119, F.S., a copy of any data in such records which is not exempt from disclosure by statute. 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 of such data shall be in accordance with the provisions of Sections 119.07(4), 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 for electronic recordkeeping hardware, software, systems, or services if such contract or obligation impairs the right of the public under state law to inspect or copy the agency’s nonexempt public records, or impairs the agency’s ability to retain the records in accordance with established records retention schedules.
3. STANDARD. In providing access to electronic records, agencies shall ensure that procedures and controls are in place to maintain confidentiality for information which is exempt from public disclosure.

(7) DOCUMENTATION STANDARDS.
(a) STANDARD. Agencies shall develop and maintain adequate and up-to-date technical and descriptive documentation for each electronic recordkeeping system to specify characteristics necessary for reading or processing the records. Documentation for electronic records systems shall be maintained in electronic or printed form as necessary to ensure access to the records. The minimum documentation required is:
1. A narrative description of the system, including all inputs and outputs of the system; the organization and contents of the files and records; policies on access and use; security controls; purpose and function of the system; update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and the location and media in which electronic records are maintained and their retention requirements to ensure appropriate disposition of records in accordance with Chapter 1B-24, F.A.C.
2. The physical and technical characteristics of the records, including a record layout or markup language that describes each file or 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 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 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 to protect the integrity of official file copies of records should meet the requirements of US Federal Information Processing Standard Publication 180-2 (FIPS-PUB 180-2) (August 1, 2002) entitled “Secure Hash Standard” (or “Secure Hash Signature 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: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf. Agencies utilizing hashing algorithms shall only use validated implementations of hashing algorithms.
3. 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 or Unicode format as prescribed by the Unicode 5.0 Standard (or successor Unicode Standard), which is hereby incorporated by reference, and made a part of this rule. This publication is available from the Unicode Consortium, P.O. Box 391476, Mountain View, CA 94039-1476, and at the Internet Uniform Resource Locator: http://www.unicode.org/book/bookform.html; 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 an electronic recordkeeping system, 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 are protected 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 electronic public records throughout their life cycle, agencies shall select appropriate media and systems which 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) STANDARD. Agencies shall not use floppy disks, audio cassettes, or VHS-format video cassettes for the storage of record (master) copies of permanent or long-term records. Permanent or long-term records on magnetic tape shall be stored on polyester-based media. Agencies shall use only previously unrecorded audio or video tape for record (master) copies of permanent or long-term audio or video recordings.
(d) STANDARD. A scanning density with a minimum of 300 dots per inch is required for scanned images created by the agency from hard copy permanent or long-term records.
(e) STANDARD. Record (master) copies of scanned images created by the agency from hard copy permanent or long-term records must be stored in accordance with a published International Organization for Standardization (ISO) open standard image format.
(f) The following factors are to be considered before selecting a storage media or converting from one media to another:
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 manufacturers); 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 back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions, human error, or other disaster. Agencies shall maintain backup electronic recording media created for disaster recovery purposes, and all preservation duplicates of permanent or long-term records, in an off-site storage facility with constant temperature (below 68 degrees Fahrenheit) and relative humidity (20 to 30 percent) controls. Storage and handling of permanent or long-term records on magnetic tape shall conform to the standards contained in Standard AES22-1997 (r2003), "AES recommended practice for audio preservation and restoration – Storage and handling – Storage of polyester-base magnetic tape" (published 1997, reaffirmed 2003), which is hereby incorporated by reference and made a part of this rule. This publication is available from the Audio Engineering Society, Incorporated, 60 East 42nd Street, Room 2520, New York, New York, 10165-2520, and at the Internet Uniform Resource Locator: http://www.aes.org/publications/standards/search.cfm. If an agency cannot practicably maintain backups and preservation duplicates as required in this section, the agency shall document the reasons why it cannot do so. Other electronic records media should be stored in a cool, dry, dark environment when possible (maximum temperature 73 degrees Fahrenheit, relative humidity 20-50 percent),
(b) STANDARD. Agencies shall annually read a statistical sample of all electronic media containing permanent or long-term records to identify any loss of information and to discover and correct the cause of data loss.
(c) STANDARD. Agencies shall test all permanent or long-term electronic records at least every 10 years and verify that the media are free of permanent errors. More frequent testing (e.g. at least every 5 years) is highly recommended.
(d) STANDARD. Agencies shall 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. 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 permanent or long-term 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 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.
(c) 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.

(13) DESTRUCTION OF ELECTRONIC RECORDS. Electronic records may be destroyed only in accordance with the provisions of Chapter 1B-24, F.A.C. At a minimum each agency shall ensure that:
(a) Electronic records scheduled for destruction are disposed of in a manner that ensures that any information that is confidential or exempt from disclosure, including proprietary, or security information, cannot practicably be read or reconstructed, and;
(b) Recording media previously used for electronic records containing information that is confidential or exempt from disclosure, including 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(1), 257.36(6) FS. Law Implemented 257.36(1)(a) FS. History–New 8-16-92, Amended 5-13-03, 5-21-08.