STATE OF TENNESSEE

Submitted to:
State of Tennessee Public Records Commission

Electronic Records Policy

State of Tennessee

Executive Sponsor
Mark Bengel
State of Tennessee Chief Information Officer
Department of Finance and Administration
Office for Information Resources

January 2010
Updated May 27, 2011

This document contains policies for uniform technical standards, procedures, and guidelines concerning the retention and disposition of electronic records in the State of Tennessee.

Table of Contents

1. INTRODUCTION

Electronic records have revolutionized the business of state government and created a growing body of digital material and data with enduring value. Preserving and providing access to the recorded evidence of work done by state agencies is a core responsibility of government. Electronic records cannot simply be put on the shelf (like paper) and forgotten—they require maintenance and an integrated electronic records and conversion strategy over long periods of time. This strategy must consider both the hardware and software infrastructures storing the data as well as the viability of the file formats, which may become obsolete over time. The stakeholders in this process of good electronic records management and custodianship are archivists, records officers, agency administrators, information officers, agency staff and, ultimately, the citizens of Tennessee.

The main purpose of this document is to define the policies for electronic records of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State.

1.1 Scope

The scope of this document is intended to cover the policies relating to the proper management of any unstructured electronic record owned, leased or controlled by the State of Tennessee to the extent permitted by law. This document applies to all state agencies in the State of Tennessee and third party contractors acting as agents of the state. By establishing the appropriate Electronic Records policy framework the State envisions maximum compliance.

1.2 Authority

The policies in this document are a joint project chartered by the Public Records Commission for the State of Tennessee (November 6, 2007) and the Information Systems Council (March 26, 2008). This joint project formed the state’s Electronic Records (eRecords) Committee, which consists of representatives from the Office for Information Resources; Records Management Division, Department of General Services (RMD); Tennessee State Library and Archives (TSLA); the Comptroller of the Treasury; and the Office of the Attorney General. These policies have been developed with input from information technology (IT) professionals; the state's Chief Information Officer (CIO); and the executive management teams within the Department of Finance and Administration; the Tennessee State Library and Archives; the Records Management Division, Department of General Services; and the Office of the Attorney General. These policies have received approval from the State of Tennessee Public Records Commission (PRC) and the Information Systems Council (ISC).

1.3 Exceptions

Notwithstanding the need for the technical standards, procedures, and guidelines presented in this document, the Electronic Records Committee (ERC) recognizes and understands the need for the immediate suspension of any stated methods for handling electronic records that can result in the modification, alteration or deletion of data that could be relevant to litigation or potential litigation. Such modification, alteration, or deletion of data could result in adverse legal consequences for the affected agency. Therefore, relevant policies contained within this document must be suspended upon the issuance of a litigation hold or preservation letter involving the affected agency's electronic records. In such instances, responsible staff should consult the independent litigation hold policies of their respective agencies.

This policy does not apply to working papers unless the working papers are subject to retention and disposition requirements established within a Records Disposition Authorization (RDA).

Working papers are defined as follows:

Those records created to serve as input for final reporting documents, including electronic data processes records, and/or computer output microfilm, and those records which become obsolete immediately after agency use or publication.

Requests for exceptions to the policies contained within this document relating to IT infrastructure or standards shall be submitted to the Office for Information Resources Information Technology Assessment and Budget Committee (IT-ABC) for disposition.

All other requests for exceptions to policy contained within this document shall be submitted to the Electronic Records Committee. The Committee will consider the justification for exception and render a disposition within a reasonable time frame.

1.4 Review

The Electronic Records Committee will review the policies contained within this document annually or as otherwise required and will communicate updates, changes, and recommendations to the Public Records Commission or Information Systems Council as appropriate for any necessary action.

1.5 Document Format

Each section will begin with a high-level policy statement for the domain that is discussed in that section. Narrative section(s) providing more detailed explanation of the requirements of the policy will follow the high-level policy statement, and may reference an Appendix, Glossary or Standard.

X. Section Name

High-level policy statement for section

OBJECTIVES

Policy name (x.x)

Policy statement

Sub-Policy name (x.x.x)

Sub-Policy statement

NARRATIVE

MINIMUM COMPLIANCE REQUIREMENTS

RESPONSIBILITIES

2. ELECTRONIC RECORDS TAXONOMY

Electronic records shall be classified in a manner consistent with their value and sensitivity to the business and operation of the state government, and their essential or non-essential nature.

OBJECTIVES

- **To determine appropriate electronic records classification, category and record series to assure the proper application of policy and best practices for treatment and storage.**

2.1 Electronic Records Classification Policy

Agencies must classify electronic records as Essential or Non-Essential.

NARRATIVE

It is expected that Electronic Records classification of Essential or Non-Essential will be recorded with the Records Disposition Authorization (RDA) associated with the relevant record series.

MINIMUM COMPLIANCE REQUIREMENTS

Implementation based on the following classification system:

- Essential – Records requiring high accessibility and retrievability, or any public records essential to the resumption or continuation of operations, to the re-creation of the legal and financial status of government in the state or to the protection and fulfillment of obligations to citizens of the state.

- Non-Essential – All other records

RESPONSIBILITIES

Agency - Responsible for all Minimum Compliance Requirements

2.2 Electronic Records Security Classification Policy

Electronic records shall be classified in a manner consistent with their value, sensitivity and essential or non-essential nature to the business and operation of the state government and those it serves or as specified by any superseding state or federal law or regulation to ensure they receive the appropriate level of protection from unauthorized disclosure, use, modification or destruction. See ISO 15489-1:2001, section 7.2.

NARRATIVE

It is expected that the Electronic Records security classification will be recorded with the RDA associated with the relevant record series.

MINIMUM COMPLIANCE REQUIREMENTS

Implementation based on the following classification system:

- **Public Record**
  A Public Record is any record, electronic or otherwise, that is not exempt from public inspection according to the provisions of state and/or federal law.
- **Confidential Record**
  A Confidential Record is any public record, electronic or otherwise, which has been designated as confidential in its entirety or portions of which have been designated as confidential by state law and/or federal law and includes information or matters or records considered to be privileged and any aspect of which access by the general public has been generally denied

Agencies may also wish to further sub-classify their electronic records, e.g., Protected Health Information (PHI) or Limited Official Use Electronic Record (LOU) within metadata.

RESPONSIBILITIES

Agency- Responsible for all Minimum Compliance Requirements

2.3 Metadata Standards Policy

Agencies must adhere to the consistent application of minimum metadata standards for Electronic Records.

NARRATIVE

Metadata is usually defined as "data about data." Metadata allows users to locate and evaluate data without each user having to discover it anew with every use. Its basic elements are a structured format and a controlled vocabulary, which together allow for a precise and comprehensible description of content, location, and value.

Each unique piece of content and versions of the content should be distinguished from all other documents in a record set, contain information that describes the document in detail, provides information on access to the data and provide information on relationships between content.

MINIMUM COMPLIANCE REQUIREMENTS

The minimal metadata elements required for classification of Electronic Records content include:

Metadata Element	**Description**
Content Subject/Title	Descriptive element to describe the content
Date Created	Date the content was created and/or modified
Format	Type of file or file extension
Content Size	Size of the File

It is **recommended** that the agency consider the following additional metadata elements for Electronic Records classified as “Essential”:

Metadata Element	**Controls**
Agency Name	Name or Code to distinguish the agency that owns the content
Unique Identifier	Unique identifier that distinguishes the record from other records
Current Version	Version of the document (Can be major 1.0 or minor 1.1)
Major Version	Version of the document (Exp.1.0)
Version Status	Active or superseded
Storage Location	Location of file (Network drive or system)
Owner	Primary owner of the content
Records Disposition Authorization	10 digit number defined by Records Management Division
Content Retention Date	Date content can be archived/destroyed
Access	Security rights to the content and type of access (Read only or Modify)
Date Last Modified	Date of the last change to the content
Last Modifier	Person who made the last change
Relation	Relationship with other content
Relation Type	Parent/Child or Sibling
Essential Nature	Essential or Non-Essential
Confidentiality	Public or Confidential

RESPONSIBILITIES

Agency:

- Record the appropriate metadata fields to be used with an Electronic Record series with the associated Record Disposition Authority (RDA).
- Record the appropriate metadata information within the Electronic Records storage system as documents are stored.

2.4 Metadata Review Policy

The <u>required and recommended metadata elements</u> will be reviewed annually by the Electronic Records Committee.

NARRATIVE

Requirements for metadata elements can change along with technology. It is imperative that each state agency ensure that the information used to describe the documents maintained is up to date with the changes in technology. The Electronic Records Committee will monitor the changes in standards and perform an annual review to assure the State adapts its metadata requirement to changes made by the International Standards Organization as appropriate.

MINIMUM COMPLIANCE REQUIREMENTS

The Electronic Records Committee will monitor appropriate International Standards Organization standards for changes in metadata standards and meet annually to incorporate those changes into policy as appropriate.

RESPONSIBILITIES

Electronic Records Committee - Responsible for all Minimum Compliance Requirements

3. FILE FORMATS

Agencies shall store electronic records in appropriate file formats.

OBJECTIVES

- **Ensure that Electronic Records are stored in formats that will assure future accessibility.**
- **Ensure that Electronic Records file formats are regularly reviewed and migrated.**

NARRATIVE

As technology constantly changes and improves, file formats can become obsolete and cause problems for future access to the records being stored. A long-term view and careful planning can overcome these risks and ensure that legal and operational requirements can be met.

3.1 File Format Determination Policy

Electronic Records should be stored in a file format that will ensure that the content of the Electronic Record is maintained for the required retention period as established by the Records Disposition Authorization (RDA).

- ***Electronic records requiring retention from creation to three years are recommended to be stored in low, medium or high confidence file formats.***
- ***Electronic records requiring retention for at least 3 years and up to 5 years must be stored in either medium or high confidence level formats.***
- ***Electronic records requiring retention for more than 5 years must be stored in high confidence file format.***

3.2 File Format Review and Migration Policy

File Formats will be regularly reviewed and migrated by the agency according to standards established in policy 3. Required and recommended file formats will be reviewed annually by the Electronic Records Committee.

NARRATIVE

File Formats will be classified according to lifecycle phase as defined below.

- **Emerging –** Formats that may be accepted as well as utilized in the industry but are new to the enterprise.
- **Current –** Tested technologies that are the current file format standard for use within the enterprise and generally accepted as standard within the industry.
- **Twilight –** Technologies that are being phased out by the enterprise but do not yet have an established end date.
- **Obsolete –** Technologies that have been phased out and cannot be used within the organization past a specific date.

MINIMUM COMPLIANCE REQUIREMENTS

The Electronic Records Committee will perform an annual review of the File Formats standards and classify each as Emerging, Current, Twilight or Obsolete. Once a format has been classified as Twilight, the agency will have three years to render the content to the current standard format.

RESPONSIBILITIES

Agency – Maintain essential content in a current or twilight standard format. Review the format standards annually. Upgrade all twilight file formats to current formats within three years.

Electronic Records Committee– Perform annual review and designate formats as Emerging, Current, Twilight or Obsolete as appropriate. Provide immediate communication to the agencies on changing standard classifications.

3.2.1 File Format Standards

High Confidence Level Formats		
Content Type	**Format**	**Lifecycle Phase**
Text	PDF-A	Current
	Plain Text	Current
	XML	Current
	Rich Text Format	Current
	Open Document Format	Current
Raster Image	TIFF	Current
Vector Graphics	None recommended	
Audio	AIFF	Current
	Standard MIDI	Current
	WAV	Current
Video	Windows Media Video	Current
Spreadsheet/Database	Delimited Text	Current
Presentation	None Recommended	
Email	Plain Text	Current
	Rich Text Format	Current
	XML	Current
Medium Confidence Level Formats		
Content Type	**Format**	**Lifecycle Phase**
Text	HTML	Current
	DTD	Current
	DVI	Current
	PDF/A-1-b	Current
	PDF	Current
	DjVu	Current
	Open Office	Current
	Computer program source code	Current

Raster Image	MrSID	Current
	BMP	Current
	FlashPix	Current
	GIF	Current
	JPEG/JFIF	Current
	JPEG2000	Current
	PNG	Current
Vector Graphics	Computer Graphic Metafile	Current
	Encapsulated Postscript	Current
	Postscript	Current
	Macromedia Flash	Current
	SVG	Current
Audio	Advanced Audio Coding	Current
	Free Lossless Audio Codec	Current
	MP3 (MPEG-1/2, Layer 3)	Current
	Ogg Vorbis	Current
	Windows Media Audio	Current
Video	Motion JPEG 2000 (ISO/IEC 15444-4)	Current
	MPEG-1, MPEG-2	Current
	MPEG-4	Current
	Ogg Theora	Current
	QuickTime Movie	Current
Spreadsheet/Database	OpenOffice	Current
Presentation	OpenOffice	Current
Email	None Recommended	Current
		Current
Low Confidence Level Formats		
Content Type	**Format**	**Lifecycle Phase**
Text	Open Office	Current
	Open Office XML	Current
	Microsoft Word	Current
	WordPerfect	Current

	Compiled / Executable Files	Current
	All other formats not listed	
Raster Image	Photoshop	Current
	All other formats not listed	
Vector Graphics	DWF	Current
	All other formats not listed	
Audio	NeXT SND	Current
	RealNetworks	Current
	SUN Audio	Current
	All other formats not listed	
Video	AVI	Current
	RealNetworks	Current
	All other formats not listed	
Spreadsheet/Database	DBF	Current
	Excel	Current
	Lotus	Current
	Microsoft Access	Current
	OpenOffice	Current
	OpenOffice XML	Current
	All other formats not listed	
Presentation	OpenOffice XML	Current
	OpenOffice	Current
	PowerPoint	Current
	All other formats not listed	
Email	Novell GroupWise	Current
	Outlook Message format	Current
	Outlook Archive	Current
	All other formats not listed	

4. PHYSICAL STORAGE POLICY

Agencies must use the proper secure storage infrastructure, processes and operational practices for systems.

OBJECTIVES

- **Ensure that content is stored on appropriate systems according to its classification**

4.1 Records Storage Policy

Electronic Records should be stored on systems appropriate to both their classification as Essential or Non-Essential and their required retention period. Use Table 4.1(a) below to determine the appropriate storage system for a given record series.

MINIMUM COMPLIANCE REQUIREMENTS

Reference the appropriate system as outlined in Table 4.1(a) when submitting a Records Disposition Authorization to the Records Management Division.

Table 4.1(a) – Electronic Records Storage System Selection Chart

	Required Retention Period		
	0-3 years	**4-9 years**	**10+ years**
Non-Essential Electronic Records	• Any appropriate storage system	• A Shared Directory on a secured and appropriately maintained file, MOSS, or SharePoint server • The State's Enterprise ECM system or a functionally equivalent ECM	• The State's Enterprise ECM system or a functionally equivalent and appropriately maintained ECM system • Tennessee State Library and Archives - permanent archival system

		system	
	0-3 years	**4-9 years**	**10+years**
Essential Electronic Records	• A Shared Directory on a secured and appropriately maintained file system, MOSS, or SharePoint server • The State's Enterprise ECM system or a functionally equivalent system	• An appropriately maintained MOSS server • The State's Enterprise ECM system or a functionally equivalent and appropriately maintained ECM system approved by the Information Technology Assessment and Budget Committee (IT-ABC)	• The State's Enterprise ECM system • A functionally equivalent and appropriately maintained ECM system approved by the Information Technology Assessment and Budget Committee (IT-ABC) • Tennessee State Library and Archives – permanent archival system

RESPONSIBILITIES

Agency - Responsible for all Minimum Compliance Requirements

4.2 Appropriate Access Control

Essential and Non-Essential records must abide by the state's Security Policies for access to Confidential and Public Records. Physical storage must provide proper access controls to the records.

MINIMUM COMPLIANCE REQUIREMENTS

Records must have an owner who is responsible for ensuring that the records abide by state records security policy as stated above.

RESPONSIBILITIES

Agency - Responsible for all Minimum Compliance Requirements

4.3 Email Appropriate Storage Policy

Email should be stored in a manner appropriate to its content and the Records Disposition Authorization (RDA) associated with that content.

NARRATIVE

Staff in government agencies frequently use email systems to distribute memos, circulate drafts, disseminate directives, transfer official documents, send external correspondence, and support various aspects of government operations. Well-designed and properly managed email systems expedite business communications, eliminate paperwork, and automate routine office tasks.

MINIMUM COMPLIANCE REQUIREMENTS

Electronic records should be classified and stored according to the policies in this document.

5. RECORDS DISPOSITION AUTHORIZATIONS

Each agency will create and maintain a Records Disposition Authorization (RDA) for each electronic records series to be submitted to the Public Records Commission.

OBJECTIVES

- **Determine and order proper disposition of state records as required by statute.**

- **Identify Records Disposition Authorizations (RDAs) for each records series stored on identified systems included in Electronic Records Plan.**

NARRATIVE

The effective management of electronic records begins with an electronic records strategy that is integrated into the Records Disposition Authorization. This will facilitate the long-term preservation of digital resources through sharing services and solutions.

- Records Disposition Authorization (RDA) shall mean the official document utilized by an agency head to request authority for the disposition of records. The Public Records Commission shall determine and order the proper disposition of state records through the approval of Records Disposition Authorizations (RDAs).

- Electronic Records must have an owner who is responsible for ensuring the record maintains its integrity and accessibility throughout the lifecycle of the document.

MINIMUM COMPLIANCE REQUIREMENTS

Agencies must complete an Electronic Records Inventory Worksheet (GS0969) that will serve as the basis for the completion of a Records Disposition Authorization (RDA) that will ultimately be submitted to the Public Records Commission.

RESPONSIBILITIES

Agency

- Must submit the Electronic Records Inventory Worksheet to the Records Management Division.

- Must submit the final Records Disposition Authorization (RDA) to the Records Management Division.

Records Management Division, Department of General Services and Tennessee State Library and Archives

- The Records Management Division, Department of General Services and Tennessee State Library and Archives shall review all submitted Records Disposition Authorizations (RDAs). After the review process, the Records Disposition Authorization (RDA) shall be submitted for approval to the Public Records Commission.

6. AGENCY ELECTRONIC RECORDS SYSTEMS PLANNING POLICY

Each agency will create and maintain an Electronic Records Plan to be submitted to the Office for Information Resources (OIR) annually in December .

OBJECTIVES

- **Ensure that the state's electronic records are appropriately stored in accordance with policy, standards, procedures, guidelines and records management best practices.**
- **Ensure that Electronic Records Plans be developed in compliance with existing Records Disposition Authorizations (RDAs) for electronic records.**
- **Ensure that new Records Disposition Authorizations (RDAs) reference an approved storage system from the Electronic Records Plan.**

NARRATIVE

The foundation of an Electronic Records Plan is an inventory of where data resides, and an analysis of the costs, the benefits, and the risks involved with each of the options that are being studied. Records management, information technology, and legal staff should all be involved in the process to make sure the plan meets the business requirements and the electronic records management strategy of the agency or department.

6.1 Electronic Records Systems Plan Submission Policy

Agencies will provide an Electronic Records Plan that will describe the storage systems utilized for electronic records.

MINIMUM COMPLIANCE REQUIREMENTS

At a minimum, the Electronic Records Plan must include the following items:

- System name
- Hardware environment description
- Software environment description
- System physical location
- Back-up procedures (include storage medium, location and frequency)
- Disaster recovery procedures
- Record series name, number, security class and classification as Essential or Non-Essential contained in the storage system

RESPONSIBILITIES

Agency – Creation and Submission of Agency Electronic Records Plan.

OIR and Electronic Records Committee – Review Agency Electronic Records Plan. Forward reviewed Electronic Records Plans to Records Management Division, General Services.

Records Management Division, General Services – Review submitted plan.

6.1.1 Agency Electronic Records Series Submission Plan

Agencies must submit a list of all agency defined electronic records series associated with each system as defined in the Electronic Records Plan.

MINIMUM COMPLIANCE REQUIREMENTS

- Record Series Title
- RDA Number
- System name and number
- File format(s)
- Retention period
- Classification as Essential or Non-Essential

RESPONSIBILITIES

Agency - Responsible for all Minimum Compliance Requirements

7. EDUCATION AND TRAINING POLICY

Office of Information Resources Division (OIR) Department of Finance and Administration will train users on compliance with the Electronic Records Policy.

NARRATIVE

This policy will become part of the regularly scheduled training of agency records managers and agency information systems personnel on records management policies contained in this document.

RESPONSIBILITIES

Office of Information Resources Division (OIR), Department of Finance and Administration

8. GLOSSARY (Appendix A)

Access Controls – access controls are used to manage proper access to data. See DOD Standard 5015.02 (04/25/2007).

Agency – agency shall mean any department, division, board, bureau, commission or other separate unit of government created or established by the constitution, by law or pursuant to law, including the legislative branch and the judicial branch to the extent that it is constitutionally permissible.

Backup (Data) **–** backup refers to making copies of data so that these additional copies may be used to restore the original in the event of a data loss.

Backup (System) **–** copies of programs, databases and other files made with the purpose of allowing the information to be restored if it is lost due to computer failure, virus infection or other unforeseen event.

Protected Health Information (PHI) **–** protected health information (PHI), under the US Health Insurance Portability and Accountability Act (HIPAA), is any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Confidential Public Record – means any public record, electronic or otherwise, which has been designated as confidential in its entirety or portions of which have been designated as confidential by state law and/or federal law and includes information or matters or records considered to be privileged and any aspect of which access by the general public has been generally denied.

Content Management Solution - the processes and workflows involved in organizing, categorizing, and structuring information resources so they can be stored, published, and reused in multiple ways. A content management system is used to collect, manage and publish content, storing the content either as components or whole documents, while maintaining the links between components. It may also provide for content revision control.

Controlled vocabulary – controlled vocabularies are used in subject indexing schemes, subject headings, thesauri and taxonomies. Controlled vocabulary schemes mandate the uses of predefined, authorized terms that have been pre-selected by the designer of the controlled vocabulary as opposed to natural language vocabularies where there is no restriction on the vocabulary that can be used.

Current – tested technologies that are the current file format standard for use within the enterprise and generally accepted as standard within the industry

DOD Standard 5015.02 – endorsed by the National Archives and Records Administration (NARA) for use by all federal agencies since 1998. It has become the de-facto standard for all Records Management Applications (RMA) and most RIM software vendors seek and obtain DOD 5015.02 certification.

Destruction – process of eliminating or deleting records, beyond any possible reconstruction (International Standards Organization 15489-1:2001 [E] Section 3.8 on page 2).

Disposition –preservation of the original records in whole or in part, preservation by photographic or other reproduction processes, or outright destruction of the records.

Electronic Records Management – Electronic Records Management is an organization's strategy for maintaining digital copies of important documents and information.

Electronic Records Plan – The document that identifies each agency's electronic records storage systems and the record series associated with said systems.

Emerging – Formats that may be accepted as well as utilized in the industry but are new to the enterprise.

Enterprise Content Management – Enterprise Content Management (ECM) is any of the strategies and technologies employed in the information technology industry for managing the capture, storage, security, revision control, retrieval, distribution, preservation and destruction of documents and content.

Essential Records – as used in this document, records requiring high accessibility and retrievability, or any public records essential to the resumption or continuation of operations, to the re-creation of the legal and financial status of government in the state or to the protection and fulfillment of obligations to citizens of the state.

File Formats – how data is organized and defined in an electronic file to be accessible by electronic systems (software).

Format standardized for input – field is formatted in such a manner that data can only be input in one manner. For example, a date field would only allow for data entry of MM/DD/YYYY.

High Confidence Level – rankings of High Confidence Levels are those file formats that can be recommended for data storage for up to 10 years. High Confidence Level File Formats must be added to the State of Tennessee Enterprise Standards list and reviewed on a yearly basis.

International Organization for Standardization – ISO is the world's largest developer of standards. It is a non-governmental organization composed of a network of the national standards institutes from 157 countries. The Central Secretariat is based in Geneva, Switzerland. The Electronic Records Committee referenced ISO Standards 15489-1:2001 and 23081-1-2006 in preparing these policies.

Limited Official Use Electronic Record (LOU) – contains information that may include, among other things, information received through privileged sources and certain personnel, medical, investigative, commercial, and financial records and material protected by the Privacy Act.

Lossless – lossless data compression is a class of data compression algorithms that allows the exact original data to be reconstructed from the compressed data.

Lossy – a lossy compression method is one where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way.

Low Confidence Level – rankings of Low Confidence Levels are for those file formats that can be recommended for data storage for up to 3 years. If any data needed for more than 3 years is currently stored in a Low Confidence Level file format, it is recommended that the data be converted to a Medium or High Confidence Level File Format.

Medium Confidence Level – rankings of Medium Confidence Levels are those file formats that can be recommended for data storage for up to 5 years. It is recommended to convert any data needed for more than 5 years currently stored in a Medium Confidence Level file to a High Confidence Level File Format.

Metadata – data about data. Structured information that describes, explains, locates, and otherwise makes it easier to retrieve and use an information resource.

The following are the metadata components and their definitions.

- Abstract – Contains a brief summary of what is contained in the document.
- Agency_Name - Contains the name of the Agency that originated the document.
- Content_Retention_Date - Specifies the date that the object must be retained, as determined by the content storage subsystem.
- Content_Size - Specifies the size (in bytes) of the captured content associated with an object.
- Creator - Specifies the short name of the user who created an object.
- Current_State - Contains the current lifecycle policy state of a Document object.
- Current_Version - Contains a Document object representing the current version in the version series.

- Date_Content_Last_Accessed - Specifies the date and time the content of a given content-carrying object was last accessed.
- Date_Created - Contains the date and time an object was created. The Content Engine stores dates and times using Coordinated Universal Time (UTC).
- Date_Last_Modified - Contains the date and time when an object was last modified. The Content Engine stores dates and times using Coordinated Universal Time (UTC).
- Document_Title - Contains a title for the document.
- ID - Contains the Global Unique Identifier (GUID) of a Content Engine object. Each object is assigned a GUID, which cannot be changed. The format of a GUID is "{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}".
- Last_Modifier - Contains the short name of the user who last modified an object.
- Major_Version_Number - Contains the current major version number for the object's version series. For two-level versioning, numbering for this value begins at 0. For single-level versioning (where all versions in the version series are major versions), numbering begins at 1. If no versioning is enabled, this property's value is 0.
- Mime_Type - Specifies the Multipurpose Internet Mail Extensions (MIME) format string for an object.
- Name – Specifies the value of the designated name property for the object.
- Object_Store - Contains an ObjectStore object representing the object store in which an object resides.
- Storage_Location - Contains a string representing the content storage location of a content-carrying object.
- Storage_Policy – Contains a Content Engine storage policy Information.
- Subject - Contains the subject of the document.
- Type_ of_ Relation – Explains the relationship between documents.
- Version_Status – Contains the current version status of a document version

Microsoft Office SharePoint Server (MOSS) – the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services. MOSS enables users to create "SharePoint Portals" that include shared workspaces, applications, blogs, wikis and other documents accessible through a Web browser.

Non-Essential – as used in this document, any public records not essential to the resumption or continuation of operations, to the re-creation of the legal and financial status of government in the state or to the protection and fulfillment of obligations to citizens of the state, and as used in this document, not requiring high accessibility or retrievability.

Obsolete – technologies that have been phased out and cannot be used within the organization past a specific date.

Office for Information Resources – the Office for Information Resources is the state agency that provides direction, planning, resources, execution and coordination in managing the information systems needs of the State of Tennessee.

Owner – the principal name of the security owner of the object.

Patch – a small piece of software designed to update or fix problems in a computer program or its supporting data. This includes fixing known errors, replacing graphics and improving the usability or performance.

Permanent Records – means those records which have permanent administrative, fiscal, historical or legal value.

Permissions – specifies the discretionary permissions for an object.

Public Record – any record, electronic or otherwise, that is not exempt from public inspection according to the provisions of state and/or federal law.

Public Records Commission – the Public Records Commission was created by statute to determine and order proper disposition of state records. See TCA 10-7-301 et seq. and Rules of Public Records Commission, 1210-1-1 (1).

Records Disposition Authorization (RDA) – shall mean the official document utilized by an agency head to request authority for the disposition of records. The Public Records Commission shall determine and order the proper disposition of state records through the approval of Records Disposition Authorizations. See Rules of Public Records Commission, 1210-1-2 (10).

Records Management – means the application of management techniques to the creation, utilization, maintenance, retention, preservation, and disposal of records in order to reduce costs and improve efficiency of recordkeeping. Records management includes records retention schedule development, essential records protection, files management and information retrieval systems, microfilm information systems, correspondence and word processing management, records center, forms management, analysis, and design, and reports and publications management.

Records Management Application – software package that manages records.

Required Metadata Element – metadata element required for input in to the Enterprise Content Management Solution.

SharePoint – a collection of products and software elements that includes, web browser based collaboration functions, process management modules, search modules and a document-management platform. SharePoint can be used to host web sites that access shared workspaces, information stores and documents, as well as host defined applications such as wikis and blogs.

State Standards – State of Tennessee Standards are guidelines/best practices, policies, procedures, products, protocols, product families, and configurations approved for use in the State of Tennessee's Enterprise Technical Architecture, known as the Tennessee Information Resources Architecture. http://intranet.state.tn.us/finance/oir/ea/.

Structured Data – structured data is organized according to a pre-determined pattern to meet a specific business need. This data is stored in electronic files and can be accessed by software specifically designed for that data or by software known as a database management system. Example: Excel Spreadsheet.

Tennessee Knowledge Network – enterprise implementation of Microsoft Office SharePoint Services that provides a platform for collaboration, web content using portals, enterprise content services, enterprise search capabilities, business forms and business intelligence.

Tennessee State Standards – see State Standards.

Twilight – technologies that are being phased out by the enterprise but do not yet have an established end date.

Unstructured Data – In computer systems, unstructured data could represent text, drawings, audio, still images, video, or some other object. Unstructured Data cannot be defined in terms of rows and columns or records, and the data cannot be examined with standard access. Example: memo written in Microsoft Word.

User Interface – the user interface of a computer program refers to the graphical, textual and auditory information the program presents to the user, and the control sequences (such as keystrokes with the computer keyboard, movements of the computer mouse, and selections with the touch screen) the user employs to control the program.

Vital Records – records essential to the continued functioning or reconstitution of an organization during and after an emergency as well as those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.

Working Documents – means those records created to serve as input for final reporting documents, including electronic data processed records, and/or computer output microfilm, and those records which become obsolete immediately after agency use or publication. These non-records include files in any format which can be considered drafts or works in progress, or which are ephemeral, temporary, or not needed for business continuity, and which are not subject to a Records Disposition Authorization (RDA).

9. REFERENCES (Appendix B)

Cain, Matthew. Toolkit Presentation: Creating an EMail Policy Document. May 18, 2007.

Chin, K. (2007). Use a Digital Preservation Plan to Manage Content for the Long Term.

Defense Technical Information Center (DTIC). DTIC Search. DoD 5015.02-STD. Electronic Records Management Software Applications Design Criteria Standard. April 25, 2007. 2008 <http://www.dtic.mil/whs/directives/corres/html/501502std.htm>.

Digital Government Presentation "Records Management (RMS) and Enterprise Content Management (ECM), What about the paper you need to keep?, October 30, 2007.

DM.review.com. 2008 <http://www.dmreview.com/glossary/u.html>.

Gartner. 2008. <http://my.gartner.com/portal/server.pt?open=512&objID=224&mode=2&PageID=466684&resId=524008&ref=QuickSearch>.

Georgia Secretary of State: Karen C. Handel. Georgia Archives. Records and Information Management Services. 2008. http://sos.ga.gov/archives/who_are_we/rims/digital_History/standards/standards%20-%20Metadata%20Standards.pdf.

International Organization for Standardization. ISO 15489 Technical Report (1 & 2). 2001 <www.iso.org>.

The Joint Interoperability Test Command. The Joint Interoperability Test Command Records Management Application. 2008 http://jitc.fhu.disa.mil/recmgt.

The Joint Interoperability Test Command. The Joint Interoperability Test Command Records Management Application. Department of Defense Electronic Records Management Software Applications Design Criteria Standards, April 25, 2007.
2008 http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf.

The Library of Congress. Digital Preservation. 2008.
http://www.digitalpreservation.gov/formats/intro/intro.shtml.

National Archives and Records Administration. Frequently Asked Questions (FAQs). About Selecting Sustainable Formats for Electronic Records. 2008 http://www.archives.gov/records-mgmt/initiatives/sustainable-faq.html.

The National Archives. National Archives and Records Administration. Tips for Scheduling Databases. 2008. http://www.archives.gov/records-mgmt/publications/tips-for-scheduling-databases.html.

National Archives of Australia. Recordkeeping Metadata Standard for Commonwealth Agencies, May 1999. 2008. http://naa.gov.au/Images/rkms_pt1_2_tcm2-1036.pdf.

Minnesota Historical Society. Minnesota's Electronic Records Guidelines.
Pages: 22-23, 50-54, 90-92. 2008
http://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/erguidelines.pdf.

Minnesota Historical Society. Minnesota Recordkeeping Metadata Standard, Version 1.2. April 2003. 2008 http://www.mnhs.org/preserve/records/docs_pdfs/rkms/mnrkms_2003.pdf.

Open Document Format *ODF Alliance.* 2008. http://www.odfalliance.org.

Public Records Commission. Rules of the Public Records Commission. Chapter 1210-1.

SC.GOV *The Official Web Site of the State of South Carolina.* South Carolina Department of Archives and History. 2008 http://www.state.sc.us/scdah/dollarsumm0122.htm.

The Sedona Conference Working Group Series. The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age. September 2005.

State Electronic Records PowerPoint, “Challenges of Electronic Records”, January 2008.

State of Tennessee INTRANET. Intranet Policies, Updated June 2003.
2008. http://intranet.state.tn.us/web_policies.html.

Tennessee.Gov: *The official Web Site of the State of Tennessee*. Acceptable Use Policy, 2-22-08, Version 1/12. 2008. http://www.state.tn.us/finance/oir/security/Acceptable-Use-Policy.pdf.

Tennessee.Gov: *The official Web Site of the State of Tennessee*. Enterprise Information Security Policies, April 4, 2008, Version 1.6. 2008. http://tennessee.gov/finance/oir/security/PUBLIC-Enterprise-Information-Security-Policies-v1-6.pdf.

Tennessee.Gov: *The official Web Site of the State of Tennessee*. Information Systems Plan Process, June 2007. 2008 http://www.state.tn.us/finance/oir/prd/ispprocess.pdf.

10. ELECTRONIC INVENTORY WORKSHEET (Appendix C)

Department of General Services
Records Management Division

ELECTRONIC RECORDS INVENTORY WORKSHEET
PART ONE

1. Department/Division _____	2. Allotment Code _____	3. Cost Center _____	4. Edison Speedchart # _____
5. Contact Person _____ Phone Number _____	6. Systems Analyst Name _____ Phone Number _____	7. ECM Analyst Name _____ Phone Number _____	
8. Date Completed _____			

DESCRIPTION OF ELECTRONIC RECORDS SERIES

9a. Electronic Record Series Title _____

b. RDA # Assigned □ Yes □ No

If yes, indicate RDA # _____ □ Paper

_____ □ Electronic

c. Indicate at which level system is used:

□ State □ Department □ Desktop

10. Classification □ Essential □ Non-Essential

11. Security Class: □ Public Electronic Record □ Confidential Electronic Record

12. Purpose of Records Series _____

13. Description of Records Series (Attach samples. Attach additional sheet for description, if needed. Include acronym, if applicable) _____

ELECTRONIC RECORDS PLAN INVENTORY

14. System Name _____	15. IT-ABC Number _____
16. Hardware Environment Description _____	
17. Software Environment Description _____	

18. Physical System Location _____

19. Backup Procedures (Include the storage medium, location and frequency) _____

20. Disaster Recovery Procedures _____

METADATA DESCRIPTION

21.

Type	Length	Format
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

INSTRUCTIONS FOR COMPLETING ELECTRONIC RECORDS INVENTORY WORKSHEET

PART ONE

1. Enter the Department and Division who has ownership of the record series.

2. Enter the Division's five-digit allotment code. (If not yet using Edison)

3. Enter the Division's cost center number or index code. (If not yet using Edison)

4. Enter the Edison Speedchart number.

5. List the name and phone number of the contact person assigned to this electronic record series.

6. List the name of the Information Systems Analyst assigned to this electronic record series.

7. List the name of the Electronic Records Content (ECM) Analyst assigned to this electronic record series and the contact phone number.

8. Indicate the date the Inventory Worksheet was completed.

9. a) List the Record Series Title
   b) Indicate if there is an assigned Records Disposition Authorization (RDA) number, and if yes, write in the number.
   c) Indicate whether the system is used at the State, Departmental or Desktop level.

10. Indicate if the record is classified as Essential or Non-Essential.

11. Indicate if the record is classified as a Public Electronic Record or a Confidential Electronic Record

12. Give a brief (approximately one sentence) description of the purpose of the electronic records series.

13. Give a brief (approximately one paragraph) description of the electronic records series. Attach samples. Attach additional sheet for description, if needed. Include acronym(s), if applicable.

14. Indicate the name of the system in which the record is stored.

15 List the IT-ABC number assigned.

16. Describe the hardware environment.

17. Describe the software environment.

18. Indicate the physical location where records are stored.

19. Describe the backup procedures in place. Include the medium, location and frequency.

20. Describe the disaster recovery procedures in place for this electronic records series.

21. For each record series included in the inventory, provide type, length and format.

ELECTRONIC RECORDS INVENTORY WORKSHEET
PART TWO

Department/Division:	**Record Series Title:**

RECORDS MANAGEMENT INFORMATION
(to be completed by Records Officer or Coordinator**)**

1. What is the date range of the record series? (Indicate oldest & newest date: mm/yy) **From** ____ / ____ **To** ____ / ____ or □ current

2. What is the current amount of storage per records series? ________ □ gigabytes □ terabytes □ other (indicate) _______

   What is the expected amount of storage accumulation per year? ________ □ gigabytes □ terabytes □ other (indicate) ________

3. Is the information shared with other state agencies or organizations outside the state? □ yes □ no

   If yes, list agencies and/or organization(s) ______________________________

4. Is data converted to paper or microform? □ yes □ no If yes, indicate the media ___________________

5. Indicate data value(s) □ Administrative □ Fiscal □ Legal □ Historical □ Evidential

6. Is the information subject to a fiscal audit? □ yes □ no If yes, indicate if required by □ Federal □ State or □ Both

7. Is the data/record required by Federal or State statute? □ yes □ no

   If yes, cite statute: **TCA:** ______________________________ Retention Period: __________ and attach copy of statute: □

   CFR: ______________________________ Retention Period: __________ and attach copy of statute: □

   Other____

8. Is the data essential to your operation? □ yes □ no

9. Is this information confidential? □ yes □ no If yes, cite statute stating confidentiality: _______________

10. How often is the data updated? __________ (daily, weekly, monthly, yearly)

11. How often is the record series referenced? (indicate number of references) ___ Current year Ref./Monthly;

___ Past Year Ref./Monthly; ___ 2 thru 5 years Ref./Monthly; ___ Over 5 years Ref./Monthly

12. Recommended Disposition of record series: The files are to be cut off at the end of each

□ calendar year □ fiscal year □ other If other, specify ________________________ then,

□ maintain in agency ___ months ___ years, then;

□ convert to (indicate media): ____

□ transfer to the State Records Center; Hold ___ years, then;

□ Destroy

□ Destroy after ____

□ Destroy when ____

□ Maintain permanently

□ Transfer to Tennessee State Library and Archives.

□ Backup tape/copy disposition will follow State-Wide RDA #10115.

□ Other (specify) ____

____

13. Justify the recommended disposition as stated above:

____

____

____

____

This Inventory Worksheet has been reviewed and approved by the Agency Records & Forms Review Committee.

Chairperson ______________________________ Division Director ______________________________

Records Officer ______________________________ ISM Director ______________________________

ELECTRONIC INVENTORY WORKSHEET

PART TWO

1. Indicate the beginning and ending (from and to) date range of the record series by completing the blanks. If the record series is still being created, use the word "current" for ending date.

2. Indicate the current volume per record series. In addition, indicate the expected annual volume accumulation per record series.

3. Indicate if the record series information is shared with other organizations by checking the appropriate box(es) and listing the organization who shares the data.

4. Indicate if the record series is converted to paper or microform by checking the appropriate box

5. Indicate the type or types of values the record series has for your organization by checking the appropriate box(es).

6. Indicate if the record series is subject to state or federal (or both) audits by checking the appropriate box(es.

7. If the data/record series is required by federal or state statute, cite the statute and the retention period in which the data/record series is to be maintained. Attach a copy of the statute to the worksheet.

8. Indicate if the record series is essential (vital) by checking the appropriate box.

9. Indicate if the record series is confidential by checking the appropriate box. If the record series is confidential, list the statute classifying the records series as confidential.

10. Indicate how often the record series is updated.

11. Indicate how often the record series is referenced.

12. Recommended Disposition of records: This item on the inventory worksheet should reflect your Records and Forms Review Committee's recommendation for the disposition of the record series based on the value of the records and how long the records are needed to conduct state business and under what condition if any the records series are to be destroyed. Indicate when the record series is to be cut off by checking either calendar, fiscal or other (if other, specify) then indicate how long the record series is to remain in the agency after it is cut off by entering the appropriate information for month(s) and year(s). Indicate if the record series will be transferred to the State Records Center and for how long. Indicate if the record series can be destroyed at this point or indicate special instructions for the disposal of the records series.

13. State or justify the reason for the recommended disposition as stated in the above question.

After the completion and review of this inventory worksheet, it is to be signed by the Records and Forms Review Committee, Chairperson, the Division Director, Records Officer and the ISM Director.

GLOSSARY OF TERMS

administrative value	defined as the importance or usefulness of records to assist the agency in performing its primary function.
archive	the act of transferring inactive electronic information to near-line or off-line storage.
Backup	Creating a copy of a computer file or data for use in case the original is lost, damaged or destroyed.
Confidential Electronic Records	any electronic record which has been designated as confidential in its entirety or portions of which have been designated as confidential by state law and/or federal law and includes information or matters or records considered to be privileged and any aspect of which access by the general public has been generally denied
data file	a computer-processable file which stores quantitative values, possibly accompanied by textual information.
DB2 Relational	the IBM mainframe relational database management system.
DIF	DATA INTERCHANGE FORMAT; spreadsheet software package which can import or export files in the worksheet format. DIF was developed and popularized by Visicorp.
diskettes	platter-shaped magnetic recording media with flexible substrates; also termed floppy disks.
EBCDIC	Extended Binary Coded Decimal Interchange Code; a coding scheme specifies bit patterns for computer processable information.
electronic records	records that contain machine-readable, as opposed to human-readable, information.
FFT	FINAL-FORM TEXT document; a document with special print formatting codes to allow you to print the document with programs other than DW4 V2.
fiscal value	defined as the importance or usefulness of records in case of financial investigation or audit.
fixed magnetic disk	the most common type of hard disk drive. A magnetic disk drive with nonremovable, rigid platters.
historical value	defined as the importance or usefulness of records to document important past events.
image file	a file which contains computer-processable images.
IMS/DB	INFORMATION MANAGEMENT SYSTEM; The IMS/DB is a hierarchical database management system.
INFOPAC	an output management software used for Report Distribution; On-line Viewing and Archival/Retrieval.
inventory worksheet	a document used to monitor and measure the usefulness of records.
legal value	the importance or usefulness of records to comply with legal requirements for maintaining information or to provide protection for an agency or State in case of litigation or investigation.
media	objects on which data can be stored. Examples include floppy disks, cd-rom, hard disk and tapes.
medium	anything (such as a magnetic disk) on which information may be stored.
Public Electronic Record	any electronic record that is not exempt from public inspection according to the provisions of state and/or federal law.
record series	a group of similar or related records that are used and filed together as a unit. A record series is generally evaluated as a unit for determining the records retention period.
rewritable optical	type of optical disk which permits erasure and overwriting of previously recorded information.

RFT REVISABLE-FORM TEXT: a form that documents are converted into before interchange can occur with other programs that support revisable form text.

source documents paper documents which contain information to be converted to electronic records.

text file a computer file which contains character-coded representations of letters of the alphabet, numeric digits, punctuation marks and other symbols encountered in typewritten documents. Text files may be created by word processing programs, electronic messaging programs or other computer software.

vital record a record necessary to continue the operation of an agency in case of disaster or emergency.

working/active Data or computer files currently in use.

write-once read many (WORM) a type of optical disk in which information can be recorded once but can be read many times.