STATE OF TENNESSEE

Submitted to:
State of Tennessee Public Records Commission

Electronic Records Policy

State of Tennessee

January 2010
Updated October 2019

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

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 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, while recognizing that this is an iterative and ongoing process.

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 Strategic Technology Solutions (STS); Records Management Division, Secretary of State (RMD); Tennessee State Library & 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 & Administration; Tennessee State Library & Archives; Records Management Division, Secretary of State; 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

The Electronic Records Committee (ERC) recognizes and understands that the policies and guidelines outlined in this document may have to be suspended in response to or anticipation of litigation. The modification, alteration, or deletion of data that could be relevant to litigation or potential litigation can have 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 guidelines 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 in TCA § 10-7-301(14) as follows:

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.

Requests for exceptions to the policies contained within this document relating to IT infrastructure or standards shall be submitted to Strategic Technology Solutions for approval.

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

1.4 Review

The Records Management Division, Secretary of State (RMD) will review the policies contained within this document as required and will communicate updates, changes, and recommendations to the Public Records Commission or Information Systems Council as appropriate for any necessary action.

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 in a way that facilitates accessibility and retrievability.

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 Organization Policy

Agencies must classify and organize electronic records according to standardized naming conventions and filing systems.

NARRATIVE

A key component of a well-maintained electronic record system is the minimization of unstructured data. This is achieved through the implementation and utilization of a well-defined record classification system. Proper and consistent record classification plays an important role in ensuring a records accessibility and retrievability over the life of its retention. It is expected that agencies will implement consistent and descriptive naming conventions and filing systems for their records.

MINIMUM COMPLIANCE REQUIREMENTS

Agencies will implement filing and naming conventions incorporating the below information and guidelines.

- **Standardized Naming Convention**
  A uniform set of rules agreed upon by an agency or division that documents how electronic files and folders should be labeled. A well-developed naming convention creates a framework for naming files and folders in a way that describes what it contains, and how it relates to other files and folders. When developing a naming convention agencies should examine their business needs and legal requirements to ensure that they develop a naming criteria that meets their needs.

It is **recommended** that agencies consider including the following information in their naming convention:

- **Project or Business Unit Name**, e.g. capital project, grants, etc.
- **Type of Data**, e.g. budget document, contract, etc.
- **Date or Date Range of records**, e.g. mmddyyyy, yy, etc.
- **Versioning,** e.g. Draft, Revision 1, Final, etc.
- **Any unique identifiers,** e.g. Case Number, File Number, Contract number, etc.
- **Avoid using special characters,** e.g. !@#$%^&*()
- **Avoid using spaces in any file names that may be accessed via web browsers**. **Instead, use hyphens or underscores between words,** e.g. File-Name, ABC_Grant_Rev1, etc.
- **For sequential numbering use leading zeros to ensure that files sort properly,** e.g. 00001, 00002, etc.
- **Avoid making file names too long**, longer file names do not work well with all types of software.

- **Standardized Filing System**

A Filing System is an organized way of structuring electronic records that allows records to be quickly identified, accessed, and located. By developing and maintaining a strict filing system agencies can avoid the increased costs associated with the unnecessary duplication of files and hours spent locating misplaced files.

It is **recommended** that agencies consider including the following information when implementing an electronic filing system:

- Structure folders/directories hierarchically: hierarchical folder structures start broadly and then become more specific as more subfolders are added. e.g. SW12_Contracts (folder), program (subfolder), and date_ contract number (sub subfolder).
- Subfolders should reflect secondary activities, e.g. programs, grants, or projects.
- Subsequent folders should be organized by calendar or fiscal years to facilitate the destruction or transfer of records to Tennessee State Library & Archives.
- Keep folder names simple to allow for easy identification.
- Include the governing Record Disposition Authorization in all top-level folders.

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 15489-1:2016.

NARRATIVE

It is expected that the electronic records security classification will be recorded with the RDA governing the record series.

MINIMUM COMPLIANCE REQUIREMENTS

Implementation based on the following classification system:

- **Public Record**
  A Public Record means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. – TCA § 10-7-301(6).

- **Confidential Record**
  A Confidential Record means any public record which has been designated confidential by statute 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. – TCA § 10-7-301(2).

Agencies may also wish to further sub-classify their electronic records to denote records containing sensitive information, e.g., Protected Health Information (PHI), Personally Identifiable Information (PII), 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.

Metadata may be stored within a digital object or in a separate database. Embedded metadata within the digital object ensures that metadata will not be lost and that it will be updated along with the document. Storing metadata also removes the need to link between the document and a separate metadata storage file. However, not all digital objects allow metadata to be embedded. In such cases it is necessary to create a means to store the metadata separately. A link must then be created between the digital object and the metadata storage system. Agencies should consult with the Division of Strategic Technology Solutions about their metadata requirements before implementing an electronic record keeping solution.

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	Unique record 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 in the associated Record Disposition Authority (RDA).
- Record all appropriate metadata information within the Electronic Records storage system as records are stored.

2.4 Metadata Review Policy

The required and recommended metadata elements will be reviewed as necessary by the Records Management Division, Secretary of State (RMD).

NARRATIVE

Requirements for metadata elements can change along with technology. It is imperative that each state agency ensure that the captured metadata is up to date with the changes in technology. The Records Management Division, Secretary of State (RMD) will monitor changes in standards to ensure the State adapts its metadata requirements as appropriate.

MINIMUM COMPLIANCE REQUIREMENTS

The Records Management Division, Secretary of State (RMD) will monitor for changes in metadata standards and incorporate those changes into policy as appropriate.

RESPONSIBILITIES

Records Management Division, Secretary of State (RMD)**-** 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 five years are recommended to be stored in low, medium, or high confidence file formats.***
- ***Electronic records requiring retention for at least five years and up to ten years must be stored in either medium or high confidence level formats.***
- ***Electronic records requiring retention for more than ten years must be stored in a high confidence file format.***

3.2 File Format Review and Migration Policy

File formats will be regularly reviewed and migrated to new file formats by the agency according to standards established in policy 3. Required and recommended file formats will be reviewed by Strategic Technology Solutions.

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 with a target end date established for completion of phase out.
- **Obsolete** – Technologies that have been phased out and cannot be used within the organization past a specific date without an exception request reviewed and approved by STS.

MINIMUM COMPLIANCE REQUIREMENTS

The Division of Strategic Technology Solutions will perform an annual review of File Format standards and classify each as Emerging, Current, Twilight or Obsolete. Once a format has been classified as Twilight, typically the agency will have three years to render the content to the current standard format.

RESPONSIBILITIES

Agency Information Systems– Maintain essential content in a current or twilight standard format. Review format standards annually. Upgrade all twilight file formats to current formats within three years. (Please note that there may be occasions where a three-year horizon cannot be set due to an unforeseen, rapid change in a given technology).

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

4. PHYSICAL STORAGE POLICY

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

OBJECTIVES

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

NARRATIVE

Regardless of physical format the necessity for state agencies to safeguard and protect their records for the full retention of the record series does not change. It is imperative that agencies work with STS to ensure that records are appropriately and adequately protected against unauthorized access, modification, destruction, or disclosure.

4.1 Records Storage Policy

Electronic Records should be stored on systems appropriate to the 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. Under no circumstances should records be maintained on employee hard drives (example C: Drive). Agencies are also not permitted to keep non-backup copies of records on external hard drives.

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

	Required Retention Period		
	0-5 years	**5-10 years**	**10+ years**
Electronic Record Storage Chart	• Any appropriate storage system	• A Shared Directory on a secured and appropriately maintained file, MOSS, or 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

RESPONSIBILITIES

Agency - Responsible for all Minimum Compliance Requirements.

4.2 Appropriate Access Control

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.

Email messages—both sent and received—that provide evidence of a government transaction are considered public records and are subject to the same legal requirements regarding access as other government records. If you have determined that an email meets the definition of a record, review the appropriate retention schedule to determine the applicable retention period. Just as with all other public records, email must be maintained and accessible throughout the life span of the record.

MINIMUM COMPLIANCE REQUIREMENTS

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

RESPONSIBILITIES

Agency - Responsible for all Minimum Compliance Requirements.

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 the appropriate Records Disposition Authorizations (RDAs) for each record series stored on systems included in the agency's 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 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 record.
- Agency Records Disposition Authorizations must be updated and revised in accordance with changes in agency business practices or state and/or federal law that affect agency recordkeeping.

MINIMUM COMPLIANCE REQUIREMENTS

Agencies must complete an Electronic Records Plan Inventory when submitting a Records Disposition Authorization (RDA). This RDA will then be sent to the Public Records Commission for approval.

RESPONSIBILITIES

Agency

- Must include Electronic Records Plan Inventory on all Records Disposition Authorization (RDA) that contain electronic records.

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

Records Management Division, Secretary of State, Comptroller of the Treasury, and Tennessee State Library & Archives

- The Records Management Division, the Comptroller of the Treasury, and Tennessee State Library & 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. EDUCATION AND TRAINING POLICY

All state agencies are responsible for ensuring that their personnel are trained on compliance with the State's Electronic Record Policy.

OBJECTIVES

- **Ensure that state agencies are educated on proper electronic record management practices.**

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

Agency - Responsible for all Minimum Compliance Requirements.

7. PRESERVATION AND ACCESS TO ELECTRONIC RECORDS

Each agency is responsible for ensuring and safeguarding public access to records for the life of the record and preparing records, as determined by an applicable RDA, for transfer to Tennessee State Library & Archives at the end of their retention.

OBJECTIVES

- **Ensure that the public's access to state electronic records is no different than their access to paper records maintained by the state.**
- **Ensure that records as determined by an applicable RDA, are stored in a way to allow for their eventual transfer to Tennessee State Library & Archives (TSLA).**
- **Ensure that State Records are stored in a way that allows for the record to be accessible, retrievable, and transferable.**

NARRATIVE

State Agencies have a responsibility to the citizens of Tennessee to ensure that state records are securely and properly maintained and preserved for the life of the record series; in the case of historical records this can mean permanently. This necessitates agencies having policies and procedures in place to ensure the accessibility, retreivability, and transferability of their records.

7.1 Electronic Records Storage Policy

Agencies will store electronic records according to the appropriate physical storage options outlined in this document and in accordance with TCA § 47-18-2901 and TCA § 10-7-121.

MINIMUM COMPLIANCE REQUIREMENTS

Each state agency shall create safeguards and procedures for ensuring that confidential information regarding citizens is securely protected on all laptop computers and other removable storage devices used by the state agency. No official copies of state records should be maintained on employee hard drives or removable storage media. All state electronic

records should be maintained in the appropriate storage format as outlined in section 4 of this document.

RESPONSIBILITIES

Agency – Responsible for all Minimum Compliance Requirements.

7.2 Electronic Records Accessibility

Agencies will store electronic records in a way that ensures the public's right to inspect State records is not infringed upon.

MINIMUM COMPLIANCE REQUIREMENTS

As required by state law access to non-confidential records must be made available for public inspection by citizens of Tennessee. The migration of a physical record to an electronic format does not relieve state agencies of this obligation. Agencies must ensure that due care is taken to maintain any information that is a public record during the time required by law for retention.

Any agency that provides remote public access to electronic records must have safeguards in place to ensure that any records inspected in this manner cannot be altered, deleted, or impaired.

RESPONSIBILITIES

Agency – Responsible for all Minimum Compliance Requirements.

7.3 Preserving and Transferring Permanent Electronic Records to Tennessee State Library & Archives

Agencies will store permanent electronic records in stable, non-proprietary formats as outlined in the table below. Agencies will transfer electronic records to the State Library & Archives in a manner that is secure and that ensures the integrity and authenticity of the data being transferred.

MINIMUM COMPLIANCE REQUIREMENTS

The following table contains preferred and acceptable formats for the long-term preservation

of common file types. If your agency's records do not fall under one of these file types, contact the State Library & Archives for additional guidance.

File Type	Preferred Formats	Acceptable Formats
Document	PDF/A	PDF, Microsoft Word
Image	TIFF, RAW	JPEG
Audio	WAVE	MP3
Video	AVI	MP4
Email	EML	MSG

Prior to transfer, records officers must complete an Electronic Records Transfer Agreement (see Appendix C), identifying key information about the records and the agency. Additionally, agencies must retain a copy of electronic records being transferred until official notification that the State Library & Archives has assumed responsibility of said records. Agencies should deliver electronic records to the State Library & Archives via external hard drive, cloud transfer, or file transfer protocol (FTP). Compact disc-read only memory (CD-ROM) or digital versatile disc-read only memory (DVD-ROM) are acceptable, though not preferred, transfer methods.

RESPONSIBILITIES

TSLA – Continually review and advise agencies on acceptable formats for storing and transferring records requiring permanent preservation.

Agency – Responsible for all Minimum Compliance Requirements.

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.

Computer Data – A series of ones and zeros (binary data) that can be created, processed, saved, and stored digitally. It does not deteriorate over time or lose quality after being used multiple times.

Confidential Public Record – means any public record which has been designated confidential by statute 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. – TCA § 10-7-301(2).

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 ISO 15489-1:2016).

Disposition – preservation of the original records in whole or in part, preservation by photographic or other reproduction processes, transfer in accordance with RDA, 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 – A large business or company.

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 format is either specified or default. Itis 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 15489-1:2016 and 23081-1:2017 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.

Low Confidence Level – rankings of Low Confidence Levels are for those file formats that can be recommended for data storage for up to 5 years. If any data needed for more than 5 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 between 5 and 10 years. It is recommended to convert any data needed for more than 10 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.

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.

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.

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.

Public Record – any record, electronic or otherwise, that is not exempt from public inspection according to the provisions of state and/or federal law. – TCA § 10-7-301(6).

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, 1210-01-.01(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, 1210-01-.02 (11).

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. See Rules of Public Records Commission, 1210-01-.02 (12).

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. https://www.teamtn.gov/content/dam/teamtn/sts/sts-documents/rptTechnologyArchitectureProducts_3.11.pd.

Standardized Naming Conventions – a uniform set of rules agreed upon by an agency or division that document how electronic records and folders should be named. A well-developed naming convention creates a framework for naming files and folders in a way that describes what they contain and how they relate to other files.

Strategic Technology Solutions – the state agency that provides direction, planning, resources, execution and coordination in managing the information systems needs of the State of Tennessee.

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 with a target end date established.

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. 2008. https://discover.dtic.mil/.

Records Management Software Applications Design Criteria Standard. April 25, 2007. http://www.dtic.mil/whs/directives/corres/html/501502std.html.

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

Georgia Secretary of State: Karen C. Handel. Georgia Archives. Records and Information Management Services. 2008. https://www.georgiaarchives.org/documents/ghrac/GHRAC_Preferred_Practices_Manual.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. http://jitc.fhu.disa.mil/recmgt.

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

Minnesota Historical Society. Minnesota's Electronic Records Guidelines. Pages: 22-23, 50-54, 90-92. 2008. https://www.mnhs.org/preserve/records/metadatastandard.php.

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.

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 Australian. Government Recordkeeping Metadata Standard Version 2.0, May 1999. 2008. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.446.5323&rep=rep1&type=pd.

Open Document Format *ODF Alliance*. 2008. http://opendocument.xml.org/odf-alliance.

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

Prairie View A&M University. Records Filing Systems. 2019. http://www.pvamu.edu/irm/wp-content/uploads/sites/45/PVAMU-Filing-System-Methodology.pdf.

Princeton University. Electronic Filing Systems. 2019. https://records.princeton.edu/records-management-manual/electronic-filing-systems.

Public Records Commission. Rules of the Public Records Commission. Chapter 1210-01. https://publications.tnsosfiles.com/rules/1210/1210.html.

SC.GOV *The Official Web Site of the State of South Carolina.* South Carolina Department of Archives and History. 2008. https://scdah.sc.gov.

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. https://www.teamtn.gov/search-results.html?q=policies.

Tennessee.Gov: *The official Web Site of the State of Tennessee*. Acceptable Use Policy, 2-22-08, Version 1/12. 2008. https://www.teamtn.gov/sts/all-services/security---risk-management-services/governance--policy---program-administration-/security-policy-documentation/administrative-user-policy--network--data-and-information-resource-access-rights-and-obligations.html.

Tennessee.Gov: *The official Web Site of the State of Tennessee*. Information Security Program, December 14, 2017, Version 1.6. 2019. https://www.teamtn.gov/content/dam/teamtn/sts/sts-documents/Enterprise-Information-Security-Policies-ISO-27002-Internal.pdf.

Tennessee.Gov: *The official Web Site of the State of Tennessee*. Information Systems Plan Process, June 2007. 2008. https://www.teamtn.gov/sts/all-services/security---risk-management-services/governance--policy---program-administration-/security-policy-

documentation/administrative-user-policy--network--data-and-information-resource-access-rights-and-obligations.html.

University of Stanford. Best practices for file naming. 2019. https://library.stanford.edu/research/data-management-services/data-best-practices/best-practices-file-naming.

State of Tennessee
Department of State
Tennessee State Library and Archives
403 Seventh Avenue North
Nashville, Tennessee 37243-0312

Electronic Records Transfer Form

Record series: RDA #:

Inclusive dates:

Total # of files:

Total volume:

Transfer method (CD, flash drive, server-to-server, etc.):

Materials transferred from:

Agency:

Name:

Title:

Address:

City: State: ZIP:

Phone:

Signature: _____

Date: _____

Materials received by:

Name:_____

Tennessee State Library & Archives

Date: _____

Folder Inventory

Folder Name	Volume	# of Files	File Formats	Date Range