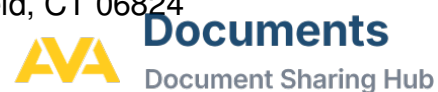




MANAGEMENT OF ELECTRONIC RECORDS

TG15-2020
May 13, 2020

NUCLEAR INFORMATION AND RECORDS MANAGEMENT ASSOCIATION
245 Sunnyridge Avenue #41, Fairfield, CT 06824



Technical guidelines developed by a committee, subcommittee, or ad hoc committee of the Nuclear Information and Records Management Association (NIRMA) represent a consensus of the members of the committee, subcommittee, or ad hoc committee with the concurrence of the NIRMA membership and Board of Directors. These guidelines are recommended procedures for establishing a program or performance of a task related to the interests of NIRMA members. Guidelines represent the consensus of the sponsoring committee on the best information based upon applicable regulatory requirements, industry standards and practical experience. A lesser amount of detail may be used to identify the areas of interface outside the scope of the document. Guidelines are not intended to be interpreted as industry standards but as suggested guidance with the understanding that companies are not obligated to use the suggested guidance.

NOTICE

This document was prepared by a committee of the Nuclear Information and Records Management Association (NIRMA). Neither this committee, NIRMA members of NIRMA, other persons contributing to or assisting in the preparation of the document, nor any person acting on behalf of these parties (a) makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this document, or (b) that the use of any information, apparatus, method, or process disclosed in this document may not infringe on privately owned rights, or (c) assumes liabilities with respect to the use of any information, apparatus, method, or process disclosed in this document.

©2020 Nuclear Information and Records Management Association. All rights reserved.

FOREWORD	vii
1. INTRODUCTION	1
1.1 Objective.....	1
1.2 Benefits.....	1
1.3 Audience.....	2
2. SCOPE	2
2.1 Context for Electronic Records Management (eRM) Programs.....	3
2.2 Key Objectives Served	4
3. DEFINITIONS	4
3.1 Audit.....	4
3.2 Backup.....	4
3.3 Content Rights Management	5
3.4 Data Element.....	5
3.5 Degaussing.....	5
3.6 Deleting.....	5
3.7 Disposition	5
3.8 Electronic Media.....	5
3.9 Electronic Records.....	5
3.10 Information System	6
3.11 Long-Term Storage.....	6
3.12 Magnetic Disk.....	6
3.13 Near-Line Storage.....	6
3.14 Off-Line Storage.....	6
3.15 On-Line Storage.....	6
3.16 Optical Character Recognition	6
3.17 Optical Disk.....	7
3.18 Program Documentation.....	7
3.19 Public Key Infrastructure (PKI).....	7
3.20 Record Retention Requirements	7
3.21 Records.....	7
3.22 Records Retention Schedule	8
3.23 Redundancy	8
3.24 Retention Period.....	8
4. CREATING ELECTRONIC RECORDS	8
4.1 Creation.....	8
4.2 Record Transformation.....	9
4.3 Capture of Hardcopy Records	9

4.4	Creation from Electronic Source Document	9
4.5	Creation from an Automated System	10
5.	AUTHENTICATING ELECTRONIC RECORDS	10
5.1	Authentication Roles	10
5.2	Authentication Methods	10
6.	TRANSFERRING AND RECEIVING ELECTRONIC RECORDS	11
6.1	Transfer Process Requirements	11
6.2	Software Application Requirements	12
6.3	Suggested Methods for Electronic Transfer and Receipt	12
6.3.1	Automated Transfer	12
6.3.2	Human-assisted Electronic Transfer of Records	13
7.	INDEXING ELECTRONIC RECORDS	13
7.1	General Indexing Guidance	14
7.2	Considerations for the Electronic Management of Metadata	14
8.	STORING AND MAINTAINING ELECTRONIC RECORDS	15
8.1	General	15
8.2	Naming Conventions	15
8.3	Formats	15
8.4	Storage of Electronic Record Content	17
8.4.1	Controlled Repository	17
8.4.2	Record Content Taxonomy	17
8.4.3	Other record storage considerations	17
8.4.4	Media Management	18
8.4.5	Records Data (Content) and Media Testing	19
8.4.6	Facility requirements	19
8.4.7	Labeling of Removable Electronic Media	20
9.	RETRIEVING ELECTRONIC RECORDS	20
10.	RECORDS RETENTION	21
10.1	Records Retention Policy	21
10.2	Records Inventory	21
10.3	Retention Processes	22
10.4	Records Retention Schedule	22

TABLE OF CONTENTS

11. DESTROYING ELECTRONIC RECORDS.....	23
11.1 General	23
11.2 Identification of Records to be Destroyed.....	23
11.3 Electronic Records Destruction.....	23
11.4 Media Containing Mixed Retention Periods.....	24
12. SECURING ELECTRONIC RECORDS.....	24
12.1 Electronic Records Security Program	25
12.2 Access Rights.....	25
12.3 Network Security	25
12.4 Content Rights Management	26
13. PLANNING FOR DISASTERS AND RECOVERING ELECTRONIC RECORDS.....	27
14. DEFINING SYSTEM AND SOFTWARE QUALITY ASSURANCE REQUIREMENTS.....	27
14.1 System Requirements	27
14.2 Software Quality Assurance.....	28
15. REFERENCES.....	29
APPENDIX A – ESTABLISHING AN ELECTRONIC RECORDS MANAGEMENT PROGRAM	33
A.1 General Principles.....	33
A.1.1 Retrievable	33
A.1.2 Intelligible	33
A.1.3 Understandable	33
A.1.4 Reliable.....	33
A.2 Policy Level Documentation.....	33
A.3 Administrative Procedures	34
A.4 Application-Specific Procedures	34
A.5 Program Organization.....	34
A.5.1 Information Manager	35
A.5.2 Information Systems Manager.....	35
A.5.3 Records Manager	36
A.5.4 Training Manager.....	37
A.6 Program Requirements Checklist.....	37
A.6.1 Examine the business process that generates the records.....	37
A.6.2 Frequency of Retrieval	38
A.6.3 Impact of Technology on Business Process	38
A.6.4 Information Analysis and Design.....	38
A.6.5 Storage Analysis.....	39
A.6.6 Data Management.....	39

APPENDIX B - FORMAT SUSTAINABILITY (SORT BY ACRONYM)	41
APPENDIX C – FORMAT TRANSFORMATION	51
APPENDIX D - CONTENT RIGHTS MANAGEMENT	52

FOREWORD

This foreword is not part of the Nuclear Information & Records Management Association Technical Guideline TG15, “Management of Electronic Records.” The Regulatory and Information Management Business Unit (RIMBU) is the responsible committee for this Technical Guideline. The following members had significant input to this document revision as it evolved for approval by the NIRMA Board of Directors.

TG15-2011 was updated to be consistent with:

- TG11, Authentication of Records and Media
- TG16, Software Quality Assurance Documentation and Records
- TG21, Required Records Protection, Disaster Recovery, and Business Continuation

Revision 2 Committee Members

Matt Henderson, STP Nuclear Operating Company, RIMBU Director

Rebecca Linder, Xcel Energy

Larry Baines, Westinghouse Columbia

Warren Martin, Yucca Mountain Project

Deborah Armentrout, Nuclear Regulatory Commission

Steve Matson, Arizona Public Service

Jeff Bartlett, Nuclear Regulatory Commission

Lynn Purdy, Bechtel SAIC

James Beasley, Sandia National Laboratories

Alan Rabe, FirstEnergy (final draft sub-committee)

Mary Binkholder, AmerenUE

Tom Reding, IBM

Robert Blem, Westinghouse

David Shipman, IBM

David Briley, Southern California Edison

Ed Springer, PSEG Nuclear

Mitchell Burke, Westinghouse

Lona Smith, South Texas Project, Units 3&4 (final draft sub-committee)

JoAnn Chovan, Chovan Associates

Lauretta Stanley, Westinghouse

Rebecca Fitzgerald, Nuclear Regulatory Commission

Roxana Taylor, Exelon Corporation

Richard Giska, Southern California Edison

Matthew Terebessy, Westinghouse

Sandy Hartman, Arizona Public Service

Michelle Smith, STP Nuclear Operating Company

Susan Hunn, Southern California Edison

Eugene Yang, KISMET Consulting, Inc. (final draft sub-committee)

Gerald Lewis, STP Nuclear Operating Company

2011 Review Team

Lauretta Stanley, Westinghouse RIMBU Director	Debra Armentrout, USNRC
Robert Acker, PPL	Jeff Bartlett, USNRC Retired
Robert Blem, Westinghouse	Chris Caston, Scana/VC Summer
JoAnn Chovan, Chovan Associates	Bill Clover, Exelon Corporation
Rae Cogar, Urenco	Rebecca Fitzgerald, USNRC
Rich Giska, Consultant	Jill Griffin, Areva
Debra Hernandez, Arizona Public Service	Beatrice Hiner, Miria Systems
Lashan Hope, Progress Energy	Jon Jedliskowski, Babcock & Wilcox
Steve Matson, Arizona Public Service	Alan Rabe, First Energy
Tonia Schneider, MNES	Michelle Smith, STPNOC
Edgar Springer, PSEG Nuclear	Jill Stern, Xcel Energy
Daryn White, Kewaunee Dominion	Eugene Yang, Kismet Consulting

2015 Revision Committee Members

Lauretta Stanley, Westinghouse
RIMBU Director

Bill Clover, Exelon Corporation

2019 Revision Committee Members

Arlene Gatti, Sargent and Lundy

Chris Sweet, Duke Energy

Gil Brueckner, General Electric

Linda Mar, Energy Northwest

Lacy Green, South Texas Project

Rich Giska, Consultant

Stephanie Price, Southern Company

Lona Smith, South Texas Project

1.0 INTRODUCTION

This guideline has been developed by the Nuclear Information and Records Management Association (NIRMA) to provide guidance concerning the management of electronic records in the nuclear industry. The initial issuance of this Technical Guideline was in 1998. Over the last decade, there has been a multitude of technology advances and innovative applications for electronic records creation, management and storage systems that span the life cycle for electronic records. In addition, on-going issues regarding acceptability of electronic records in legal proceedings continue to challenge Information and Records Managers. Thus, the Regulatory and Information Management Business Unit (RIMBU) within NIRMA has undertaken this update to TG15.

1.1 Objective

This revision to TG15 is intended to assist the NIRMA constituency and the nuclear industry in developing tactical and strategic plans for improving the overall effectiveness of electronic records management (eRM) programs. It is not a prescriptive document; rather, it incorporates a combination of experience, best practices and evolving technologies that can be leveraged to enhance individual eRM programs and support compliance with regulatory and legal obligations.

The guidance provided herein should be considered with respect to individual programs and applied where appropriate. The guidance is focused on many aspects of electronic records, e.g., format, media, storage, quality assurance, security and overall programmatic issues. The specific objective for inclusion of these topics is to encourage assessment and application of the applicable guidance to enhance existing eRM Programs throughout the nuclear industry.

It must be noted that this guideline does not address certain operational aspects of electronic files or data, e.g., source code file management, transaction system data, document distribution or uncontrolled copies of electronic records, or structured data such as that found in databases. In addition, it does not cover the subject areas of Enterprise Content Management or Electronic Content Management. These topics are candidates for future NIRMA Technical Guidelines.

1.2 Benefits

NIRMA is recognized as the authority in the nuclear industry for information and records management. Consideration and application of these guidelines will provide a solid foundation for any eRM Program in the nuclear industry.

Additional benefits will be realized through the definitions and use of common terms that will allow clarity of issues and enable better collaboration and sharing of experiences and alternative solutions among industry colleagues. The guidelines reflect the collective knowledge and experience of seasoned industry professionals and represents the best guidance and direction available in the nuclear industry.

The details provided in the Technical Guideline (TG) will also allow benchmarking of individual eRM Programs with the industry's best practices and enable assessment of current and evolving technologies for application in individual programs. Individual assessments should consider local plant issues and environments with a goal of incorporating best practices or upgraded technologies that will improve the overall effectiveness of the individual Program.

1.3 Audience

This guideline content and structure is intended to support the Information Management and Records Management professionals within the nuclear power industry. Specifically, it is directed to personnel who manage the requirements for the creation, maintenance, use, and disposition of electronic records.

It is also suitable for use in communication and collaboration with the Information Technology management personnel as it provides a set of common elements and terms that will facilitate development of effective solutions.

The guidance herein may also be applied to other nuclear-related operating facilities or other highly-regulated industry facilities. It provides an effective framework from which individual eRM programs relevant to other industries can be developed.

2.0 SCOPE

Electronic records may exist in any electronic format (e.g., Portable Document Format [PDF]), and on various media (e.g., magnetic disk), capable of being read by computer system application software and peripheral subsystems. This guideline addresses the complete life cycle of electronic records and their information processing environments.

The body of this document is structured as a process flow. The activities consist of:

- Creating
- Authenticating
- Transferring and Receiving
- Indexing
- Storing and Maintaining
- Retrieving
- Retaining
- Destroying

Information processing environment topics include:

- Security
- Disaster Planning and Recovery of Electronic Records
- System and Software Quality Assurance Requirements

These activities are dependent on having a records management program that contains elements for addressing electronic records already in place in accordance with Appendix A, Establishing an Electronic Records Management Program.

2.1 Context for Electronic Records Management (eRM) Programs

This guideline is premised on the structure and content of eRM Programs as illustrated in Figure 1, Electronic Records Management Context which presents the key components and their interrelationships.

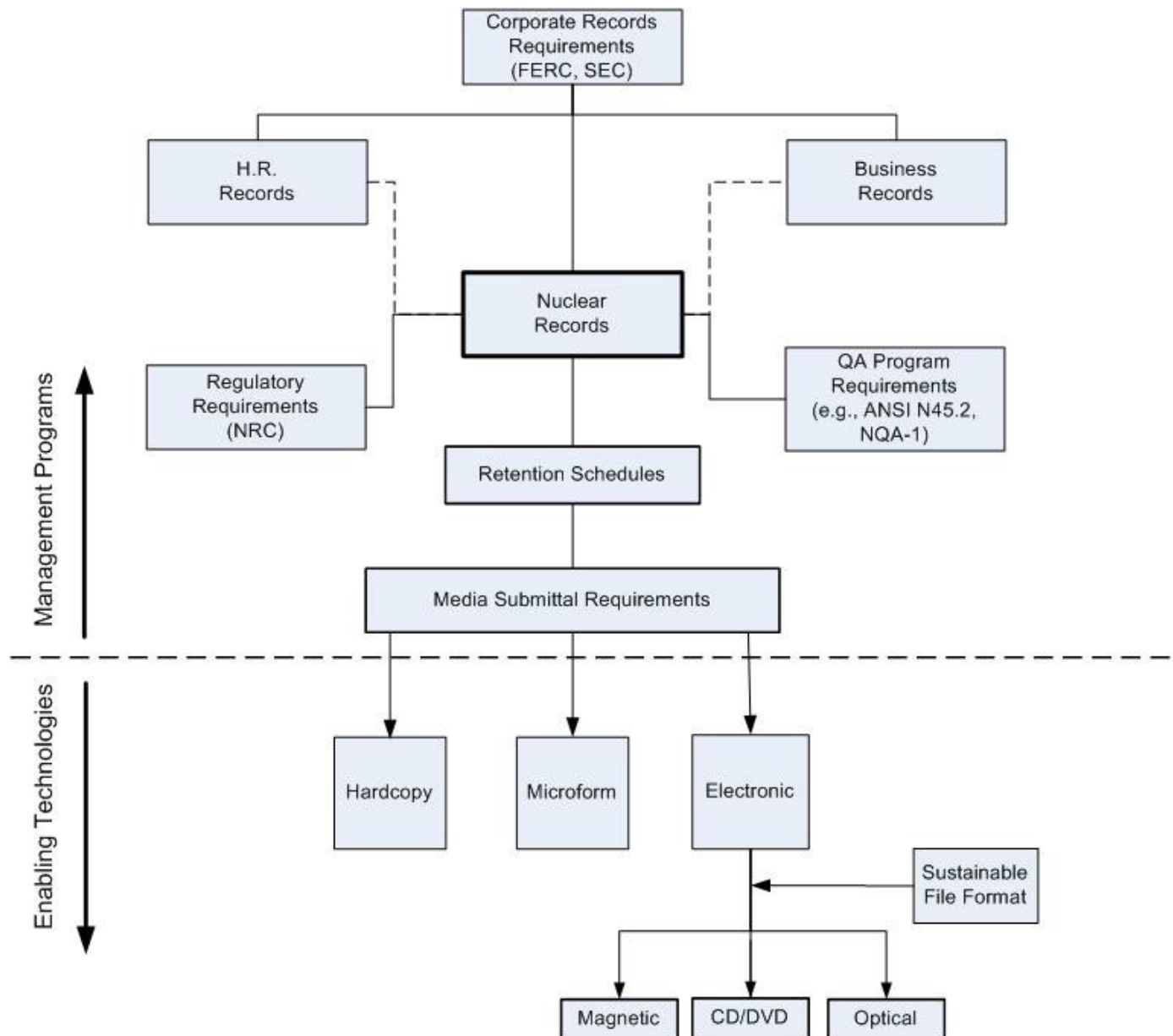


Figure 1: Electronic Records Management Context

2.2 Key Objectives Served

The guidance provided within this TG may be applied to achieve various objectives for an Electronic Records Management (eRM) Program in an organization. This begins with the fundamental element of establishing the eRM Program and associated policies, procedures, roles and responsibilities.

The structure, scope and control measures of any eRM Program should recognize the inherent complexities of electronic records. The guidance in this TG will enable organizations to understand the nature of relevant risks and assess the options for managing them.

Application of key principles provided in this TG will support achieving specific targeted goals, e.g.:

- Effective eRM Program for Quality Records in the nuclear industry that supports commitments to regulatory requirements for records management.
- RM Program that will produce “trustworthy” records (information that has been reviewed and authenticated, and that there are processes that assure the integrity is maintained to ensure that the information remains dependable and reliable) that can withstand legal scrutiny and enable admission of electronic records for legal proceedings.

This TG is not intended to provide a specific solution to any individual organization’s eRM Program. Rather, it provides as much relevant information as possible with the objective that an organization will be enabled to make prudent business and knowledge-based decisions for its own eRM Program.

3.0 DEFINITIONS

3.1 Audit

a planned and documented activity performed to determine by investigation, examination, or evaluation of objective evidence the adequacy of and compliance with established procedures, instructions, drawings, and other applicable documents, and the effectiveness of implementation. An audit should not be confused with surveillance or inspection activities performed for the sole purpose of process control or product acceptance.

3.2 Backup

A collection of data stored on (usually removable) non-volatile storage media for the purpose of recovery in case the original copy of the data is lost or becomes inaccessible.

3.3 Content Rights Management

Access control technologies used to limit usage of digital files, media or devices. These technologies control access to protect sensitive information from unauthorized access. It may also refer to restrictions associated with specific instances of digital works or devices. This is also known as Information Rights Management, Digital Rights Management, Enterprise Rights Management, or Enterprise Digital Rights Management.

3.4 Data Element

A combination of characters or bytes referring to one separate item of information, such as name, address or age.

3.5 Degaussing

To make the magnetic media effectively non-magnetic by neutralizing the magnetism, thus effectively destroying the stored information on the magnetic media.

3.6 Deleting

The process of removing, erasing, or obliterating recorded information from a medium, especially a magnetic tape or disk. Sometimes called scratching or erasing.

3.7 Disposition

Disposition is the action(s) taken when records are no longer needed in their current environment. These actions may include transfer to alternative storage facilities or disposal of records per their retention schedule.

3.8 Electronic Media

Any type of recording medium such as magnetic disk, fixed content/server-based storage, diskette, optical disk, compact disc, DVD disc, tape, or other electronic storage devices.

3.9 Electronic Records

Records stored in a form that only a computer can process. Also called machine-readable records or Automatic Data Processing (ADP) records, electronic records include:

- Content - The text, data or substance material of the record. Refers to what is captured within a record, such as drafts showing corrections, blank and completed forms, or a memo with the “to” and “from” information.
- Context - The data about the data (metadata). May include data which describe the system or application in which the data was captured as well as how the data was captured. Refers to what makes the record meaningful and describes its relationship to other records, such as approval, agreement, etc.

- **Structure** - The form and format of the data content. Refers to how information is organized which greatly impacts our ability to understand it.

3.10 Information System

A program designed to collect, process, store, retrieve, transmit and disseminate information in accordance with defined procedures, whether automated or manual.

3.11 Long-Term Storage

Long-term is defined as "long enough to be concerned with the impacts of changing technologies, including support for new media and data formats, or with a changing user community. Long-term may extend indefinitely." (ISO 19005-1:2005). Long Term is synonymous with "lifetime" as used in ANSI N45.2.9.

3.12 Magnetic Disk

Magnetic Disk Technology with content protection mirroring (every object is written to two devices at the same time) which eliminates the potential for copying corrupt data from one device to another. The data integrity checker recalculates content addresses of all objects and compares them to the original content address to ensure that no corruption exists. This checker runs continuously in the background and replaces the need for electronic file image sampling. Mirror technology also provides the ability for "self-healing" by automatic replacement of corrupted objects.

3.13 Near-Line Storage

A device which provides unattended access to information recorded on electronic media, such as optical disks or magnetic tape.

3.14 Off-Line Storage

This is the electronic storage of information that is not under the direct control of a computer. Data on media such as a magnetic tape or removable diskette are not directly accessible for immediate processing by a computer when it is not inserted into a tape or disk drive that is connected to the computer.

3.15 On-Line Storage

This is the electronic storage of information that is under the direct control of a computer. Data is usually on a magnetic disk, and is directly accessible for immediate processing by a computer.

3.16 Optical Character Recognition

Optical character recognition (OCR) is the mechanical or electronic translation of images of handwritten, typewritten or printed text (usually captured by a scanner) into machine-editable text. All OCR systems involve not only a scanner for creating a digital image of the text, but also sophisticated software for analyzing and converting those images into machine-editable text. It also includes digital image processing.

3.17 Optical Disk

Optical Disk is a non-contact, random-access disk tracked by optical laser beams and used for mass storage and retrieval of digitized text and graphics. Optical Disk is sometimes called an optical digital disk or optical digital data disk. There are three recording types: Read Only (commonly referred to as WORM - Write Once Read Many), Recordable, and Re-Recordable. Common media types of optical disks include the Compact Disk (CD) and the Digital Versatile Disk (DVD).

3.18 Program Documentation

Recorded information used to maintain the integrity of electronic records. This includes the information required to plan, develop, operate, maintain, and use electronic records and software. Examples include company policy, system specifications, file specifications, code books, program manuals (e.g., procedures) and user guides.

3.19 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a method that provides a mechanism for securely issuing and distributing public keys. The means of distribution for the public key is a certificate, which binds a public key with information about the user to which it is issued. Certificates are signed by a PKI component known as a certification authority (CA). The CA vouches for the identity of the entity to which the certificate is issued. This infrastructure is also considered to include the:

- Private Key – meaning the key of a key pair that is used to create a digital signature.
- Public Key – meaning the key of a key pair that is used to verify a digital signature.

3.20 Record Retention Requirements

Industry standards, legal rules of evidence, federal regulations, insurance requirements, and other federal, state, or local laws or regulations which provide general or specific guidance on particular records to be created and maintained by an organization.

3.21 Records

Information regardless of physical form or characteristics, appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the organization. Examples of where this information may reside are: books, papers, maps, photographs, machine readable electronic files, or other documentary materials.

3.22 Records Retention Schedule

A listing that indicates the record description and the length of time records must be retained to fulfill legal, regulatory, insurance, or company operating requirements. This listing provides the authority for the final disposition of records.

3.23 Redundancy

The duplication of critical components and data within a system with the intention of increasing reliability of the system and accessibility of the data, usually in the case of a backup or fail-safe.

3.24 Retention Period

The period of time an official recordkeeping copy is to be retained and retrievable as a result of regulatory, legal, or business requirements. The record may be either the original or reproduced copy.

4.0 CREATING ELECTRONIC RECORDS

Electronic information can be found on a variety of electronic media such as hard disks, network disk drives, optical disks and magnetic tapes among others. Digital objects (e.g., electronic documents, electronic records) may include text, graphics, sound or video recordings generated from a variety of software/hardware configurations. Complex documents may be composed of multiple computer files stored in multiple locations across the computing environment.

4.1 Creation

Records are created from documents that the business unit has either developed or received under an approved process. Information created or stored electronically does not of itself make that information a record. It must meet the requirements of the established records management program. Electronic records are created in the following three ways, which are discussed further below:

- Capture of Hardcopy Documents
- Creation from source document
- Creation from external automated system

Quality and accuracy of electronic document files submitted are the responsibility of the originator and may be checked by the records personnel, (e.g., file can be opened, content is legible, and the file is in a sustainable format). Quality standards are established by the records organization to support business needs and/or requirements.

The originator may be required by the records program to supply additional attributes and/or information for records turnover.

4.2 Record Transformation

Documents may be created in black and white, or grayscale or color. When they become records a determination must be made whether they need to be transformed. How it is accomplished may be affected by software, hardware or other cost considerations. For example, a Word document converted to PDF will be a smaller file size. Additionally, use of graphics may be discouraged due to adverse impact on file size. However, for many companies this is not a significant consideration.

A document may be in various formats during its lifecycle including transformation from hardcopy or microform to electronic format. The transformation process must be detailed in appropriate documentation. The transformed document must be verified to contain the same information as the original per quality assurance requirements. See **Section 8.3** for a discussion on the use of sustainable formats when considering record transformations.

4.3 Capture of Hardcopy Records

Hardcopy (paper files) need to be scanned to create an electronic record. The scanning should be conducted using documented standards and procedures. Scanning may result in an image, or it may create a document utilizing optical character recognition (OCR) or field recognition.

The scanning process includes visually inspecting the quality of the image and verifying the content has not changed. Verification should ensure the intent of the document is not changed if scanning color hardcopy content to black and white image.

Verification testing may be done on an established sample basis. After quality and accuracy of the electronic file are ensured, the original may be destroyed if not restricted by regulatory, business or insurance requirements.

Scanning of a record that is the property of another entity could be a violation of copyright law and should only be done with permission of the owner.

4.4 Creation from Electronic Source Document

Documents may be created in any electronic format. However, if they are not created in a long-term, sustainable format, as identified in **Section 8**, then a transformation is required. Business process needs may dictate which format to implement for creation, use and storage.

Even though an authenticated copy is needed for records purposes, an original file in native format may be needed for purposes of future revision. Only the latest copy of this file needs to be kept. A good practice is to develop a system of retaining these current native files, while ensuring that historical files are not kept in duplication of records.

4.5 Creation from an Automated System

Electronic documents may be created by an automated system. Such documents would meet the requirements of **Section 4.4**.

Transaction-based, structured data systems (e.g., work management system) must provide records-based information.

An effective approach would be to have the transaction-based system provide an output report, such as a table – such a format provides the context, content, and structure, and can then be saved in a format that meets sustainability criteria. In the event that a transaction system cannot provide such an output, then that system (hardware, software, application, and database) needs to be subject to the requirements of this TG.

5.0 AUTHENTICATING ELECTRONIC RECORDS

Authentication is the approval of a document that will be kept as a record. The basis is provided in 10 CFR 50 and implemented through ANSI N45.2.9 or ASME NQA-1.

NIRMA TG11, Authentication of Records, provides additional detail. The following paragraphs describe methods of authentication.

5.1 Authentication Roles

The basic purpose of authenticating a document is to formalize the completion of a process. Authentication must have the following attributes:

- Content authentication: This signature(s) attests to the accuracy of the content.
- Record authentication: This signature is the final approval and completes the document as a record.

A single signature may suffice for both attributes. Signatures are protected so that they cannot be falsified or altered without detection.

5.2 Authentication Methods

The types of authentication methods providing evidence of approval may be demonstrated by one of the following:

- Wet Signature (pen to paper, signature, or initials) – a type of legal authentication that is required by a specific law and must be maintained in this format. When allowed, the approved hard copy record that contains a wet signature can be scanned and converted into an electronic format using a controlled process maintaining the chain of custody and then stored as an electronic record.