



TG15-2025

MANAGEMENT OF ELECTRONIC RECORDS

Revision 4

APPROVED:

Signed by:

A handwritten signature in blue ink that reads "Bruce Walters". The signature is written over a horizontal line.

79C6BA2103FF49D...

Bruce Walters, CRM/NS, President

9/16/2025

Date



Documents

Document Sharing Hub

INTENT AND DISCLAIMER STATEMENT

Technical Guidelines developed by a Committee, Subcommittee, or Ad Hoc Committee of the Nuclear Information 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. Guidelines are recommended procedures for establishment of 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, other persons contributing to nor 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 assumes liabilities with respect to the use of any information, apparatus, method, or process disclosed in this document.

©2025 Nuclear Information and Records Management Association. All rights reserved.

1.0 SCOPE..... 11

2.0 DEFINITIONS..... 14

3.0 ESTABLISHING AN ELECTRONIC RECORDS MANAGEMENT PROGRAM.. 24

4.0 ELECTRONIC RECORDS PROCESS GUIDANCE..... 30

4.1 CREATING ELECTRONIC RECORDS 30

4.2 AUTHENTICATING ELECTRONIC RECORDS..... 32

4.3 TRANSFERRING AND RECEIVING ELECTRONIC RECORDS 34

4.4 INDEXING ELECTRONIC RECORDS 36

4.5 STORING AND MAINTAINING ELECTRONIC RECORDS..... 39

4.6 RETRIEVING ELECTRONIC RECORDS..... 46

4.7 RECORDS RETENTION..... 47

4.8 DESTROYING ELECTRONIC RECORDS..... 49

4.9 SECURING ELECTRONIC RECORDS..... 51

5.0 DISASTER PLANNING AND RECOVERY OF ELECTRONIC RECORDS..... 55

5.1 DISASTER RECOVERY TEAM..... 55

5.2 PLAN DEVELOPMENT 56

5.3 PREVENTION PLANNING..... 57

5.4 SYSTEM BACKUP AND DISASTER PLANNING..... 57

5.5 FOREWARNING CONSIDERATIONS 58

5.6 RESPONSE AND RECOVERY 59

5.7 POST-DISASTER ANALYSIS 60

5.8 TESTING AND MAINTENANCE 60

6.0 SOFTWARE QUALITY ASSURANCE REQUIREMENTS..... 61

7.0 ARTIFICIAL INTELLIGENCE (AI) 62

8.0 REFERENCES..... 63

APPENDIX A – ELECTRONIC RECORDS MANAGEMENT SYSTEM..... 71

APPENDIX B - BEST PRACTICES AND CONSIDERATIONS..... 74

APPENDIX C - FORMAT SUSTAINABILITY (SORT BY ACRONYM)..... 78

APPENDIX D – FORMAT TRANSFORMATION 80

APPENDIX E - CONTENT RIGHTS MANAGEMENT..... 81

REVISION SUMMARY
REVISION 4 DESCRIPTION
• Reformatted in compliance with AD01, Revision 9. • Added additional descriptions regarding Figure 1.1 found in Section 1.0. • Added additional definitions (Section 2.0) • Establishing an electronic records program was moved from the appendix to being part of the main document (See Section 3.0) • Edited, expanded, or removed statements or otherwise clarified guidance in Section 4.0 • Incorporated guidance from TG11 (Section 4.2), TG16 (Section 6.0) and TG21 (Section 5.0). • Added a section on Artificial Intelligence for information; NIRMA does not currently have specific guidance on its use in information management or records management. • Appendices Changes: ○ New Appendix A provides a general description of a electronic records management system ○ New Appendix B provides lessons learned considerations with a cross reference to particular sections of this TG ○ Appendix C now contains the sustainability matrix and has been updated to reflect current evaluations ○ Appendix D provides electronic object transformation guidance ○ Appendix E contains content rights management information

FOREWORD

[This Foreword is not part of 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 with respective approvals by the NIRMA Board of Directors.

Review Committee Members	
Matt Henderson, STP Nuclear Operating Company, RIMBU Director	Rebecca Linder, Xcel Energy
Deborah Armentrout, Nuclear Regulatory Commission	Warren Martin, Yucca Mountain Project
Larry Baines, Westinghouse Columbia	Steve Matson, Arizona Public Service
Jeff Bartlett, Nuclear Regulatory Commission	Lynn Purdy, Bechtel SAIC
James Beasley, Sandia National Laboratories	Alan Rabe, FirstEnergy (final draft subcommittee)
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 Revision 2 Committee Members	
Lauretta Stanley, Westinghouse RIMBU Director	Debra Hernandez, Arizona Public Service
Debra Armentrout, Nuclear Regulatory Commission	Beatrice Hiner, Miria Systems
Robert Acker, PPL	Lashan Hope, Progress Energy
Jeff Bartlett, Nuclear Regulatory	Jon Jedliskowski, Babcock & Wilcox

NIRMA

TG15
Revision 4
Page 6 of 83

2011 Revision 2 Committee Members	
Commission	
Robert Blem, Westinghouse	Steve Matson, Arizona Public Service
Chris Caston, SCANA/VC Summer	Alan Rabe, FirstEnergy
JoAnn Chovan, Chovan Associates	Tonia Schneider, MNES
Bill Clover, Exelon Corporation	Michelle Smith, STP Nuclear Operating Company
Rae Cogar, Urenco	Edgar Springer, PSEG Nuclear
Rebecca Fitzgerald, Nuclear Regulatory Commission	Jill Stern, Xcel Energy
Richard Giska, Consultant	Daryn White, Kewaunee Dominion
Jill Griffin, Areva	Eugene Yang, KISMET Consulting

2015 Review Committee Members	
Lauretta Stanley, Westinghouse RIMBU Director	Bill Clover, Exelon Corporation

2020 Revision 3 Committee Members	
Gil Brueckner, General Electric	Linda Mar, Energy Northwest
Arlene Gatti, Sargent and Lundy	Stephanie Price, Southern Company
Richard Giska, Consultant	Lona Smith, South Texas Nuclear Operating Company
Lacy Green, South Texas Nuclear Operating Company	Chris Sweet, Duke Energy

2025 Revision 4 Committee Members	
Eugene Yang, KISMET Consulting (subcommittee chair)	Meg Milligan, Hanford, US Dept of Energy
Gil Brueckner, GE Hitachi Nuclear Energy	Stephanie Price, Southern Company
Richard Giska, Consultant	Lona Smith, South Texas Nuclear Operating Company
Sandra Miller, Devereaux Consulting	

ABSTRACT

A commercial nuclear facility is required to establish and maintain a quality assurance (QA) program, per Title 10 of the Code of Federal Regulations (CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

Criterion XVII, Quality Assurance Records, states that, in part, "Sufficient records shall be maintained to furnish evidence of activities affecting quality." Over the course of 60-plus years of nuclear facility operations, the volume of recordkeeping has grown exponentially to not only provide evidence of plant operations, but also support capital improvements and, eventually, decommissioning activities.

Management of electronic records became a key method in support of plant effectiveness and efficiency. Since 1998, the Nuclear Information and Records Management Association has promulgated guidance for electronic records. This guidance was provided through several Technical Guidelines (TGs), coordinated in areas such as records processing, authentication, file format sustainability, systems integration, software configuration management, and backup/disaster recovery planning.

This Technical Guideline consolidates and streamlines such guidance into a single source, while also adding new guidance for emergent and anticipated issues.

INTRODUCTION

On December 6, 1953, President Dwight D. Eisenhower presented his “Atoms for Peace” speech to the United Nations General Assembly. The speech inspired a focus on peaceful uses of atomic energy. It catalyzed the United States’ commitment to design, construct, and operate electric power plants using nuclear reactors. The “Atoms for Peace” program led to the creation of regulations for the use of nuclear power which culminated in Title 10, Energy, of the Code of Federal Regulations (10 CFR). 10 CFR created the U.S. Nuclear Regulatory Commission (NRC), and is the basis for the NRC’s regulatory actions. A plant must receive a license to operate, and as part of that license, it must have a QA program based on 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities”, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”. This appendix cites 17 criteria for such a program; one such is Criterion XVII, “Quality Assurance Records”.

The industry wanted to have a say on how to implement the Appendix B requirements, so standards organizations, such as the American National Standards Institute (ANSI) and the American Society of Mechanical Engineers (ASME) developed, respectively, ANSI N45.2.9, “Requirements for Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants,” and ASME NQA-1, “Quality Assurance Requirements for Nuclear Facility Applications”, Requirement 17. Through these standards, more specificity was provided on the “what’s” and high-level “how’s”, including defining record types and their related retentions.

As the means to managing records medium have evolved from paper to microfilm and now to electronic, each of the medium has presented opportunities and challenges. This guideline (NIRMA TG15, “Management of Electronic Records”) was 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 (TG) was in 1998. At that time, the following TGs were also produced:

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

These four TGs constitute the electronic records guidance provided by NIRMA. These have been cited, in their various versions, by the U.S. Nuclear Regulatory Commission, to provide guidance in the use of electronic technologies in managing quality assurance records. These are found in Regulatory Guide 1.28, “Quality Assurance Program Criteria (Design and Construction)”, Revisions 5 and 6, and Regulatory Guide 1.33, “Quality Assurance Program Requirements (Operation)”, Revision 3.

Since then, information technology has continued to advance with 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 have continued to challenge Information and Records Managers. To meet these needs, NIRMA continued to either re-affirm or update the TGs as necessary. Then, finally, as part of the current update process, the decision was made to consolidate all the pertinent NIRMA electronic records guidance into this particular TG.

OBJECTIVE

This revision to NIRMA TG15 is intended to assist the NIRMA constituency, and the nuclear industry, in developing strategic and tactical 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 technology description that can be leveraged to enhance individual ERM programs and support compliance with regulatory and legal obligations.

The guidance provided here should be considered with respect to individual programs and applied where appropriate. It is focused on many aspects of electronic records, (e.g., format, media, storage, QA, security and overall programmatic issues).

The specific objective is to encourage assessment and implementation of the relevant guidance to enhance existing ERM programs throughout the nuclear industry.

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, sharing of experiences, and alternative solutions among industry colleagues. The guidance contained in this TG reflects 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 this TG also allow benchmarking of individual ERM programs with the industry's best practices. It will also enable individual assessments of current and evolving technologies for application. Such assessments should consider local plant issues, continuous improvement objectives, commitments, and environments with a goal of incorporating best practices or upgraded technologies that will improve the overall effectiveness of the individual program.

AUDIENCE

The content and structure of this TG are 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 Information Technology and Digital Engineering management personnel as it provides a set of common elements and terms that will facilitate development of effective solutions. In addition, concepts in this guidance can assist in communicating with personnel from other plant functions (such as Engineering, Operations, Maintenance, etc.) to identify and assess new records; methods for capture and systems integration; and advising on retention needs.

The guidance may also be applied to other nuclear-related operating facilities, development of new nuclear projects, or other highly-regulated industry facilities. It provides an effective framework from which individual ERM programs relevant to other industries can be developed.

1.0 SCOPE

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

1.1 CONTEXT

This guideline is premised on the various regulatory obligations, structure and content of ERM programs as illustrated in Figure 1, Electronic Records Management Context. This illustration presents the key components and their interrelationships.

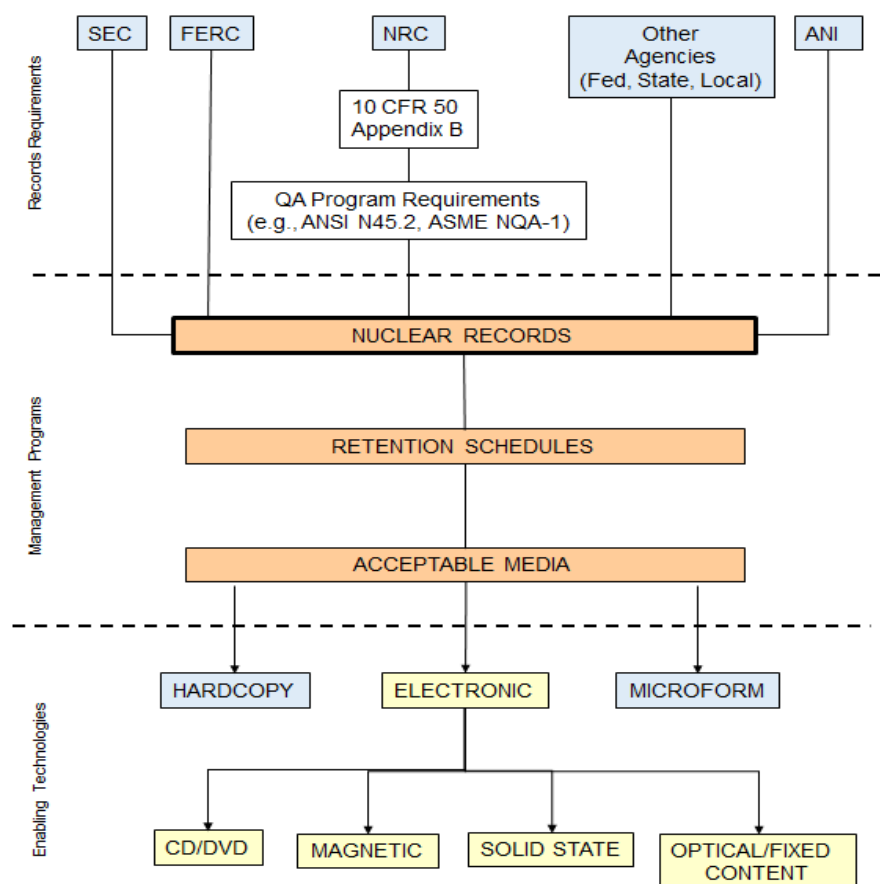


Figure 1. Electronic Records Management Context

A nuclear power facility is typically part of a larger company that is providing the electric energy into the market. To that end, various federal, state, and local agencies with regulatory authority subject that company (and subsequently, the facility) to recordkeeping requirements. These include:

- Securities and Exchange Commission (SEC), which requires publicly traded companies to maintain records related to business operations;
- Federal Energy Regulatory Commission (FERC), which regulates the interstate transmission of natural gas, oil, and electricity;
- Nuclear Regulatory Commission (NRC), which regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements.
- American Nuclear Insurers (ANI), is a voluntary joint underwriting association consisting of some of the leading insurers and reinsurers from the United States, based on the requirement that large commercial reactors licensed by the NRC must maintain financial protection for the benefit of the public in the event of a nuclear accident. Several long-term record keeping requirements come from ANI.
- Other agencies include the Environmental Protection Agency, the Department of Energy, state-based nuclear regulatory departments, and local ordinances pertaining to public and worker safety.

1.2 PROGRAM ELEMENTS OVERVIEW

The ERM program is a sub-component of a nuclear facility's records management program. This begins with the fundamental element of establishing the ERM Program and associated policies, procedures, roles and responsibilities. The elements listed below contain guidance that can augment the facility's records management program.

- General principles
- Policy level documentation
- Administrative procedures
- Application-specific procedures
- Program organization
- Program requirements checklist (See **Appendix B**)

1.3 PROCESS ELEMENTS OVERVIEW

The process guidance is structured according to a record's lifecycle. The activities consist of:

- Creating/Transforming
- Authenticating
- Transferring and Receiving
- Indexing
- Storing and Preserving
- Retrieving
- Retaining
- Dispositioning (e.g., further retention, transferring, destroying)

1.4 INFORMATION PROCESSING ENVIRONMENTS OVERVIEW

Information processing environment topics include:

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

1.5 KEY OBJECTIVES

The guidance provided within this TG may be applied to achieve various objectives for an organization's ERM program.

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, such as.:

- An effective ERM program for quality records in the nuclear industry that supports commitments to regulatory requirements for records management. This not only includes storing the electronic records on appropriate storage media, but assuring the integrity, quality, and retrievability of records per the retention requirements (which, for the vast

majority of records is “life of plant”, which could be 60-100 [or more] years into the future).

- The overall RM Program will maintain “trustworthy” records through management processes that review and authenticate the information to ensure that the information remains dependable and reliable, thus withstanding legal scrutiny and enabling 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, informed, and knowledge-based decisions for its own ERM program.

2.0 DEFINITIONS

2.1 ARTIFICIAL INTELLIGENCE (AI)

The term Artificial Intelligence (AI) refers to a machine-based system that can go beyond defined results and scenarios and has the ability to emulate human-like perception, cognition, planning, learning, communication, or physical action. For a given set of human-defined objectives, AI can make predictions, recommendations, or decisions influencing real or virtual environments. These systems use machine- and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action.

2.2 AUTHENTICATION

The act of attesting that the information contained within a document is accurate, complete, and appropriate to the work accomplished. The quality of being valid, authentic/genuine.

2.3 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.

2.4 BACKUP

A copy of selected computer files, programs, or data written to a duplicate media or another media or system for use if the original is lost, damaged, or destroyed. Active and inactive files are typically backed up. Back-up copies of files must be geographically separated from the originals to fulfill disaster recovery objectives and to fulfill requirements for duplicate storage of electronic records.

2.5 BACKING UP

The act of copying selected computer files, programs, or data to another media or system for use if the original is lost, damaged, or destroyed.

2.6 BUSINESS CONTINUITY PLAN (BCP)

The plan that describes the ability of an organization's vital/essential functions to operate during and/or following any system outage conditions. This spans any situation from simple system outage, server disruption/maintenance through full emergency/disaster conditions.

2.7 CLOUD COMPUTING

Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis. Cloud computing allows an organization to lease computer systems and services from predominately computer service organizations. These organizations pool resources to serve multiple customers via the internet, thus relieving the customers of buying, storing, supporting, and maintaining equipment and software themselves.

2.7.1 Infrastructure as a Service (IaaS)

This type provides infrastructure resources, such as servers, network, operation systems, and data storage, from a location(s) where the services are provided to many clients on usually shared resources.

2.7.2 Platform as a Service (PaaS)

This type provides frameworks that developers can use to build custom applications and deliver their applications over the internet. It provides the data serving, storage and management resources to the developer so they do not have to own the software and hardware and manage the technology. The customer is utilizing those resources as a service and relying on the provider to maintain the equipment, software resources, security and technology.

2.7.3 Software as a Service (SaaS)

This type refers to cloud-based software that is hosted by a software vendor who provides the software service to multiple customers from shared datacenters of equipment and services. The shared data centers may or may not own the infrastructure being used by the software.

2.8 CONFIGURATION MANAGEMENT

The discipline applied to the identification, management, and change control of software configuration items, including source code, integrated modules, and executable code, as well as the documentation that identifies and describes the application or system. Integration of the application or system with other systems is also part of configuration management, such as purpose, function, and points of integration.

2.9 CONTENT RIGHTS MANAGEMENT

Access control technologies that are 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 (e.g., preventing printing of digital content or copying text). This is also known as Information Rights Management, Digital Rights Management, Enterprise Rights Management, or Enterprise Digital Rights Management.

2.10 DATA ELEMENT

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

2.11 DEGAUSSING

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

2.12 DELETING

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

2.13 DISASTER

A sudden, unplanned, calamitous event that creates an inability on the part of an organization to perform critical business functions for some period of time.

2.14 DISASTER RECOVERY PLAN

An approved document containing management policy and provides the necessary activities required to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. This should include: a) identifying and prioritizing records, b) a reasoned approach to recover and/or reconstruct an organization's records, and c) establish procedures for the resumption of business operations in the event of a disaster.

2.15 DISPOSITION

Disposition is process of determining if a record that reaches its end of required retention should be retained for business needs or any other basis for keeping the record. Such action(s) can be taken when records are no longer needed in their current environment (e.g., hardcopy or electronic). These actions may include transfer to alternative storage facilities or disposal of records per their retention schedule.

2.16 ELECTRONIC MEDIA

Any type of recording medium such as magnetic disk, fixed content/server-based storage, diskette, optical disk, compact disk (CD), digital versatile disk (DVD), tape, or other approved electronic storage devices.

2.17 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 the following elements:

2.17.1 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.

2.17.2 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.

2.17.3 Structure

The form and format of the data content. Refers to how information is organized which greatly impacts our ability to understand it. This includes the metadata that comprises a digital signature, when applicable.

2.18 ELECTRONIC RECORDS SYSTEM

Any information system that captures, produces, processes, and/or stores records by using a computer.

2.19 INFORMATION SYSTEM

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

2.20 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 and in ASME NQA-1.

2.21 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.

2.22 NEAR-LINE STORAGE

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

2.23 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 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.

2.24 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.

2.25 OPTICAL CHARACTER RECOGNITION (OCR)

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.

2.26 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 CD and DVD.

2.27 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.

2.28 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:

2.18.1 Private Key

The key of a key pair that is used to create a digital signature.

2.18.2 Public Key

The key of a key pair that is used to verify a digital signature.

2.18.3 Preservation of Digital Certificates

Documents signed electronically do not need to have their certificates of authenticity preserved as long as the record exists. However, a process must be established to validate the Digital Signature using the certificate provided. Once this is done and statused as such in the records system, then any future loss of the certificate does not invalidate the record. Any changes or additions to the document after final signature shall be addressed with a supplement. An approved process for making changes to documents electronically is described in approved procedure/policy.

2.29 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.

2.30 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.

2.30.1 Quality Assurance (QA) Record

A Quality Assurance (QA) Record is a completed document that furnishes evidence of the quality of items and/or activities affecting quality. A document is considered a quality record when the document has been authenticated via the originator's signature, stamp, initials, or other approval, and dated by authorized personnel. Quality records may be originals or reproduced legible copies and may be lifetime or non-permanent records. Types of record media may include paper, electronic, or specially processed media such as radiographs, photographs, negatives and microfilms. QA Records shall be legible, identifiable and retrievable.

2.30.2 Non-Quality Assurance (Non-QA) Record

A record that does not meet the definition of a QA record, but which documents the completion of an activity deemed important to meet regulatory, industry or corporate requirements

2.31 RECORDS RETENTION SCHEDULE (RRS)

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.

2.32 RECOVERY

The activities associated with restoring resources or operation following a disruption in normal operations.

2.33 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.

2.34 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 the reproduced copy.

2.34.1 Lifetime Record

Quality records are classified as lifetime if they meet one or more of the following:

- Records that would be of significant value in demonstrating capability for safe operation of a nuclear power plant.
- Records that would be of significant value in maintaining, reworking, repairing, replacing, or modifying a safety-related item.
- Records that would be of significant value in determining the cause of an accident or malfunction of a safety-related item.
- Records that provide required baseline data for in-service inspection of a nuclear power plant.

2.34.2 Permanent Record

A record which has a permanent or lasting administrative, legal, fiscal, research or historical value and therefore must be retained and preserved indefinitely

2.34.3 Temporary Record

A record identified for disposal, either immediately or after a specified retention period. Temporary records are considered to have short-term administrative value.

2.35 SERVICE LEVEL AGREEMENT (SLA)

A service-level agreement (SLA) defines the level of service expected from a service provider (e.g., internal IT resources, external vendor), where the metrics are defined by which service is measured, as well as remedies or penalties should the agreed-upon service levels not be achieved.

2.36 SITE

A "ready to use" data processing facility which usually consists of a structurally hardened building, environmentally controlled room, raised flooring, reliable/redundant power supply. Site must contain computer hardware, software, expanded telecommunications links, operating systems software, and applications programs.

2.36.1 Cold Site

A "ready to use" data processing facility that does not maintain data and systems in "systems-ready" state. Instead, it requires a specified time to initiate recovery. A cold site is considered to be less expensive than a warm or hot site due to lower staffing and less-responsive data access requirements.

2.36.2 Warm Site

A "ready to use" data processing facility where data is constantly replicated between the host and provider data centers, but the computer resources at the warm site are "lights out" until the customer declares an event. This can be seen as a cost savings over a hot site as the customer will not have to pay for computer resources which are not being used. There are very little resources required to just keep the data between sites in sync.

2.36.3 Hot Site

A "ready to use" data processing facility where data is constantly replicated between the host and provider data centers, and the system can be diverted to the site with very limited actions, preferably automated on loss of the primary site. A hot site maintains data and systems in "systems-ready" state, provides immediate recovery, and is usually considered to be more expensive than a cold or warm site because of increased staffing and more-responsive data access requirements.

2.37 SOFTWARE

Includes computer programs, procedures, operating systems, applications, firmware, rules, documentation and data.

2.38 SOFTWARE LIFE CYCLE (SLC)

The phases of a given software application or system from initial concept through development, operation, maintenance and retirement. Phases may be sequential or iterative.

2.39 SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

Those phases of the SLC that focus on the initial conception, requirements, design, build, test, and release to production (operations). Key software development life cycle (SDLC) methodologies include waterfall, agile, and scrum.

2.40 SOFTWARE QUALITY ASSURANCE (QA)

Software QA is the planned and systematic pattern of all actions necessary to provide adequate confidence that a software product conforms to established functional and technical requirements. Thus, the scope of software QA includes both management and technical aspects of software development and maintenance.

2.41 SOFTWARE QUALITY ASSURANCE PLAN (SQAP)

A documented systematic approach that identifies all actions necessary to provide adequate confidence that the subject application or system conforms to identified requirements and can be maintained throughout its SLC.

2.42 SOFTWARE VERIFICATION

The process of determining whether the products of a given phase of the computer development process fulfill the expectations established during the previous phase. For example, it is intended to check that a product, service, or system meets a set of design specifications.

2.43 STATUS

The state in which a record exists.

2.43.1 Active

Active records are documents (both hardcopy and electronic) which are still actively being used and have not yet attained their retention limit. They are usually accessed on a frequent basis (daily, weekly, or monthly).

2.43.2 Obsolete

Obsolete generally refers to a record that is no longer active.

2.43.3 Superseded

A record that has been removed from use and replaced by another document. Typically, these are records that represent controlled documents.

2.43.4 Void

A record which is void is of no legal effect whatsoever; an absolute nullity.

2.44 VALIDATION

The process of evaluating a computer program at the end of a development process to support compliance with functional requirements. For example, it is intended to ensure a product, service, or system results in a product, service, or system that meets the operational needs of the user.

2.45 VITAL RECORDS

Records essential to the continued functioning or reconstitution of an organization during and after an emergency. Also includes those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities. Sometimes called “essential records,” vital records include both emergency-operating and rights-and-interests records. Vital records considerations are part of an agency’s records disaster prevention and recovery program. QA records are considered part of a Vital Records program.

3.0 ESTABLISHING AN ELECTRONIC RECORDS MANAGEMENT PROGRAM

This section addresses the principles, policy, procedural recommendations, and organization and program requirements for establishing an electronic records management program. The electronic records programs should be considered a part of the overall records program and involves program elements and organizational responsibilities for implementing the program elements.

3.1 KEY PRINCIPLES**3.1.1 Retrievable**

Records must be organized and indexed so that the user, who may not know the exact title or nature of the record, will be able to locate it using logical search parameters. The records must be retrievable for their full retention period.

3.1.2 **Intelligible**

Records must be readable and reproducible for their entire life cycle. Because hardware and software technologies may change over the lifetime of a record, maintenance and configuration control measures must be applied to the storage and retrieval systems to ensure the continued readability of the records.

3.1.3 **Understandable**

An electronic record of an activity or process need not reflect the original form or format of the data. However, these records must be maintained in such a way to be rendered into a human readable format and provide a clear understanding of the content, context and structure of the original record.

3.1.4 **Reliable**

Systems and processes must be developed to preclude alteration or corruption of the data. Process documentation governing the entire lifecycle of the record must be developed and approved by the records authority. Training should be conducted for all affected personnel, commensurate with their role and responsibility regarding records.

3.2 **POLICY**

The organization responsible for managing records should identify and define the program requirements for electronic records. This should also include what constitutes an electronic record (i.e., the creation method, the criteria [form, format, structure]) and emphasize that maintenance of, and access to, such records must meet federal, state, local, regulatory, business, and other legal retention requirements. These requirements should receive concurrence by legal counsel.

The policy should also explicitly state that the official medium is electronic, of which the types include magnetic, solid state, digital tape, etc. Given that the medium is electronic, the original record resides on that medium, and it is that record that must be referenced when performing work or decision-making. (A hardcopy of that electronic record may be used if the policy explicitly states that the hardcopy represents a record copy and can be used).

The electronic records program should be declared the official program to be followed for all applicable activities associated with the creation, electronic storage, retention, and disposition of electronic records. As stated earlier, the ERM program is governed by the overall RM program, which should be structured to meet all records, be they in hardcopy, microform and electronic.