**Document Title:** Requirements of a Trustworthy Electronic Records Preservation System in a College or University Setting

**Document Number:** 2.1

**Version:** Draft for Public Comment

**Date:** 08/16/05

**NHRPC Grant Number:** 2004-083
I. Organization

1. Organization
   Outline of the organization of this document.

2. Introduction
   Definition of the purpose of this document and articulation of its basic assumptions.

3. Form of the requirements
   The scope and syntax of the requirements for a trustworthy recordkeeping system, including sample requirements with explanations of each section of a requirement entry.

4. Records Preservation System Requirements
   Lists and definitions of the requirements for a records preservation system. This section organizes the requirements into six primary sections (based on OAIS activities) and __ categories of requirements within those primary sections:

   1. Ingest
      1.1. Manage transfers
      1.2. Accept all types of electronic records
      1.3. Check electronic records contained in a transfer

   2. Archival Storage
      2.1. Store records reliably (including Protection from Loss or Corruption)

   3. Data Management
      3.1. Information About Records

   4. Administration
      4.1. Protection from Loss or Corruption
      4.2. Reporting capability & Event log
      4.3. System administration

   5. Preservation Planning
      5.1. Manage preservation planning framework
      5.2. Manage templates

   6. Access
      6.1. Use Rights
      6.2. Discovery and Delivery

5. Degrees of Obligation for each Requirement
   Definitions of the three requirement levels for implementation of each requirement.
II. Introduction

This document describes the features, behaviors, and qualities of a trustworthy records preservation system at a college or university, written as requirements that are necessary in order to preserve electronic records and ensure their continued accessibility and authenticity over time in the preservation repository as the creating technologies become obsolete. A preservation system is the whole of the activities and processes involved in the technical stabilization and physical and intellectual protection of resources through time.

In contrast to some notions about the preservation, the process of preserving an electronic record goes well beyond keeping it safely in storage. The process of digital preservation begins with the initial act of transfer and storage and extends all the way through reproduction of the record.

Because the nature of recordkeeping and records preservation systems are so similar (and in some juridical contexts considered identical) the requirements for records preservation systems draw substantially, but not wholly, from the major policy literature cited in Requirements of a Trustworthy Electronic Recordkeeping System in a College or University Setting, especially in the areas of archival storage, administration, and access. Thus, all of the sources cited in Requirements of a Trustworthy Electronic Recordkeeping System have been consulted in the preparation of these requirements, although not necessarily cited specifically. Those sources are:

- Indiana University, Requirements for Electronic Records Management Systems
  In this document referred to as: Indiana

- University of Pittsburgh, Functional Requirements for Evidence in Recordkeeping
  In this document referred to as: Pitt

- Center for Technology in Government, Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records
  In this document referred to as: CTG

- IDA Programme of the European Commission, Model Requirements for the Management of Electronic Records
  In this document referred to as: MoReq

- Public Records Office, Functional Requirements for Electronic Records Management Systems
  In this document referred to as: PRO

- InterPARES I Project, “Requirements for Assessing and Maintaining the Authenticity of Electronic Records,” in The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project
  In this document referred to as: InterPARES
• U.S. Department of Defense, *Design Criteria Standard for Electronic Records Management Software Applications* (DoD 5015.2-STD)
  In this document referred to as: DoD

• International Organization for Standardization, *ISO 15489-1: Information and documentation—Records management*
  In this document referred to as: ISO

• San Diego Super Computer Center at the University of California, San Diego, *Preserving the Electronic Records Stored in a Records Management Application* (PERM Project)
  In this document referred to as: PERM

• Health Information Privacy Protection Act
  In this document referred to as: HIPPA

In addition, we have surveyed the preservation system requirements literature and selected what we believe to be the 7 most applicable to the university archives community. This literature is much less standardized than the recordkeeping system requirements literature, consisting mostly of more vague research best practices statements. In the last 2 years, the situation has been altered dramatically by the landmark work completed by the National Archives and Records Administration’s Electronic Records Archives Program Management Office. This grand and detailed statement of responsibilities must be considered the most significant work of its kind. The full list of the preservation system requirements documents includes:

• National Archives and Records Administration Electronic Records Archives Program Management Office, *Electronic Records Archives Requirements Document* (RD)
  In this document referred to as: NARA

• Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System*
  In this document referred to as: OAIS

• San Diego Super Computer Center, *Preserving the Electronic Records Stored in a Records Management Application*
  In this document referred to as: PERM

• Research Libraries Group, *Trusted Digital Repositories: Attributes and Responsibilities*
  In this document referred to as: TDR

• IBM and Koninklijke Bibliotheek, *Preservation Requirements in a Deposit System: IBM/KB Long Term Preservation Study*
  In this document referred to as: KB
• Yale University Library, Requirements Document for the Rescue Repository
  In this document referred to as: RR
III. Form of the requirements

The requirements for a records preservation system described in Section IV are for either the Application itself or for People, Institution, Procedure, or Infrastructure. No requirements are expressed as requirements for a Records Preservation System. As Records Controls themselves impose requirements on records preservation systems, the document does not include requirements for any Controls. Each requirement includes only one of these five records preservation system components. While some requirements may pertain in some way to multiple components, every requirement in this report only contains the most relevant component.

The requirements in this report are organized into 6 sections. Each section has numerous levels subsections. All of the requirements are nested within the subsections.

Each requirement will have a unique number, the text of the requirement itself, and a citation to one or more of the research projects discussed in Section II. The text of the requirement itself will contain one of the five Record Preservation System Components (Application, Infrastructure, Institution, People, or Procedures), a degree of obligation (MUST, MUST NOT, SHOULD, SHOULD NOT, or MAY), and then a description of the actual requirement. See Figure 2.

Figure 2. Example Requirement
IV. Records Preservation System Requirements

1. Ingest

According to the OAIS Reference Model Ingest, “accepts Submission Information Packages (SIPs) from Producers (or from internal elements under Administration control) and prepares the contents for storage and management within the archive. Ingest functions include receiving SIPs, performing quality assurance on SIPs, generating an Archival Information Package (AIP) which complies with the archive's data formatting and documentation standards, extracting Descriptive Information from the AIPs for inclusion in the archive database, and coordinating updates to Archival Storage and Data Management.”

1.1. Manage transfers

1.1.1. Accessioning

1.1.1.1. An Institution MUST register transfers with a unique id.

[Yale A.5–A.6]

1.1.1.2. An Application MUST persistently link unique registration ids to applicable transferred records.

1.1.1.3. An Institution MUST provide for transfer of legal custody of records to the archives.

[NARA 1.3]

1.1.1.4. An Application MAY automate the implementation of submission agreements.

[NARA 1.6–7]

1.1.2. Capture Information about Records

1.1.2.1. An Application SHOULD be capable of automatically extracting metadata for the records it captures from a recordkeeping application.

[Indiana 1.6.1; MoReq 6.1.6, 6.1.14; Yale B.5; NARA 3.3–3.5]

1.1.2.2. An Application MUST allow people to manually enter metadata that cannot be automatically extracted from the records captured from a recordkeeping application.

[Indiana 1.6.3; MoReq 6.1.9; PRO A.2.38, PERM 12; NARA 3.3]

1.1.2.3. Procedures MUST provide for the creation of necessary metadata
during the capture process that did not exist before capture (including descriptive, technical, and contextual metadata necessary to document ingest).

[MoReq 6.1.9; PRO A.2.38, PERM 12, Indiana 1.2.3; Pitt 8a; MoReq 6.1.2, 6.1.3; ISO 7.2.1.b; NARA 3.3]

1.1.2.4. An Application MUST maintain any links between ingested records and their metadata.

[Indiana 1.2.3; MoReq 6.1.3; ISO 7.1.c]

1.2. Accept all types of electronic records

1.2.1. An Institution MAY accept all data types in which electronic records are written.

1.2.2. An Application MUST to ingest data files in the digital formats in which they were received, as specified by submission agreements.

[NARA 7.2]

1.2.3. An Application SHOULD accept transfers via physical media.

[NARA 14.1]

1.2.4. An Application SHOULD accept transfers electronically.

[NARA 14.2]

1.2.5. An Application SHOULD accept electronic records that are composed of more than one digital component.

1.2.6. An Application MUST be capable to interact with all of the institution’s recordkeeping applications.

[Indiana 1.6.2; MoReq 6.2.1; PRO A.2.2; NARA 1.10]

1.3. Check electronic records contained in a transfer

1.3.1. An Institution MUST confirm that the transfer is authorized.

[NARA 1.2]

1.3.2. An Application SHOULD be able to confirm that a transfer is authorized by a submission agreement.

[NARA 1.2]

1.3.3. An Application MUST be able to validate that a records transfer complies
with the submission agreement (terms and conditions of transfer).
[NARA 14.4]

1.3.4. An Application MUST confirm the success of a file transfer (verification).
[NARA 14.3]

1.3.5. An Application SHOULD be able to technically validate that records components conform to technical file format standards.
[Yale B.4; NARA 5.8]

1.3.6. An Institution SHOULD provide feedback to the producer on the success or failure of the transfer.
[Yale B.4]

1.3.7. An Application MUST be able to technically validate the metadata it creates or captures.
[Indiana 1.6.4; MoReq 6.1.1]

1.3.8. Procedures SHOULD provide for the intellectual validation of the metadata the records preservation system creates or captures during ingest.
[Indiana 1.6.4; MoReq 6.1.1]

2. Archival Storage
According to the OAIS Reference Model Archival Storage, “provides the services and functions for the storage, maintenance and retrieval of AIPs. Archival Storage functions include receiving AIPs from Ingest and adding them to permanent storage, managing the storage hierarchy, refreshing the media on which archive holdings are stored, performing routine and special error checking, providing disaster recovery capabilities, and providing AIPs to Access to fulfill orders.”

2.1. Store records reliably (including Protection from Loss or Corruption)

2.1.1 Intrusion Detection and Response

2.1.1.1 Procedures MUST provide a reasonable guarantee that records are protected from tampering.
[Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPPA 45CFR164.306(a)(2)]

2.1.1.2 Procedures MUST prescribe periodic software security updates.
[HIPPA 45CFR164.308(a)(5)(ii)(A)]
2.1.2 Disaster Preparation

2.1.2.1 Procedures SHOULD provide for the automated backup of the preserved records and preservation metadata.
[MoReq 4.3, 4.3.1, 9.1.2-3; PRO A.9.11, A.9.17; Dod c2.2.9.1]

2.1.2.2 An Application MUST NOT hinder automated backup of the institution’s records.

2.1.2.3 Procedures SHOULD articulate the actions needed to be undertaken during primary system failure.
[Pitt 2d; MoReq 4.3.5; HIPPA 45CFR164.308(a)(7)(i), HIPPA 45CFR164.308(a)(7)(ii)(C)]

2.1.2.4 Infrastructure SHOULD allow for backups to be stored at geographically distant locations.
[PRO A.9.12; DoD c2.2.9.2; Yale C.2]

2.1.2.5 An Application SHOULD provide facilities for restoring data from backup data and returning the data stores to a state prior to disaster.
[Pitt 4d; MoReq 11.3.5, 4.3.3, 4.3.4; PRO A.9.14-16; DoD c2.2.9.3, c2.2.2.9.3.1-2, c2.2.9.4-5; HIPPA 45CFR164.308(a)(7)(ii)(B); NARA 9.2.3]

2.1.3 Manage the Preservation Process

2.1.3.1 Media Decay (manage media)

2.1.3.1.1 An Institution SHOULD develop a physical storage media tracking system.
[NARA 11.1]

2.1.3.1.2 Procedures MUST allow for storage media to be maintained in an appropriate physical environment.
[MoReq 11.7.1; ISO 8.3.3]

2.1.3.1.3 Procedures SHOULD allow for periodic checks for media deterioration.
[MoReq 11.7.2, 9.1.5; NARA 11.6–10]

2.1.3.1.4 Procedures MUST allow for the migration of records from one storage media to another in a manner that preserves the recordness of the records.
2.1.3.1.5 An Application MUST NOT modify electronic records to accommodate physical storage media. [NARA 11.2]

2.1.3.1.6 An Application MAY provide the automated capability to move electronic records to different media to accommodate new technology. [NARA 11.1]

2.1.3.1.7 An Institution SHOULD possess tools for recovery of electronic records from failed media. [NARA 11.4]

2.1.3.2 Hardware and Software Obsolescence

2.1.3.2.1 An Application MUST have the capability to store copies of electronic records [NARA 9.1]

2.1.3.3 Transformation

2.1.3.3.1 An Application MUST provide the capability to transform any ingested data file to a different, more persistent format. [NARA 7.5-7.6]

2.1.3.3.2 An Application MUST persistently link the format versions of the same records together. [PRO A.2.12; NARA 9.1.3]

2.1.3.3.3 Upon any transformation, an Application SHOULD NOT involve an irreversible conversion from one data format to another [Yale A.9]

2.1.4 Destruction of Records

2.1.4.1 An Application MUST provide the capability to destroy any electronic record [NARA 1.5]
3. Data Management

According to the OAIS Reference Model Data Management, “provides the services and functions for populating, maintaining, and accessing both Descriptive Information which identifies and documents archive holdings and administrative data used to manage the archive. Data Management functions include administering the archive database functions (maintaining schema and view definitions, and referential integrity), performing database updates (loading new descriptive information or archive administrative data), performing queries on the data management data to generate result sets, and producing reports from these result sets.”

3.1 Information About Records

3.1.1 Unique Identifier

3.1.1.1 An Application MUST uniquely identify the records it maintains.

[Pitt 6c; MoReq 7.1; PRO A.9.3; DoD c2.2.1.4, c2.2.4.1; PERM 15; Yale A.5]

3.1.2 Copies of Records (Versions)

3.1.2.1 An Application MUST manage the relationship between the copies of records components in the system.

[Indiana 1.2.8; DoD c2.2.3.18–c2.2.3.20; NARA 7.4]

3.1.2.2 An Application MUST manage the relationship between all copies of records components to their corresponding records.

[NARA 7.4]

3.1.2.3 An Application MAY support identification of the authoritative version (master copy or preservation copy) of a record component in the system.

[IP A.7]

3.1.2.4 An Application MUST document any changes of a record component from the point of ingest.

[InterPARES B.3]

3.1.2.5 An Application MUST document items removed from the preservation system, including filenames, timestamps and a person identifier.

[Yale D.3]

3.1.3 Location Tracking
3.1.3.1 An *Application* MUST be able to track the location of its records.  
[MoReq 4.4.1]

3.1.3.2 An *Application* MUST track a record’s unique identifier, current location, time of movements, and the person responsible for the movements.  
[MoReq 4.4.3; ISO 9.8.3]

3.1.4 Demonstration of Controls over Records Transfer, Maintenance, and Reproduction

3.1.4.1 An *Institution* SHOULD demonstrate it has created and maintains a reasonable access criteria and it has successfully implemented the criteria.  
[InterPARES B.1; ISO 8.3.6]

3.1.4.2 An *Application* SHOULD facilitate the creation, maintenance, and distribution of documentation to support a demonstration of controls over records transfer, maintenance, and reproduction.  
[InterPARES B.1; NARA 7.5.1-7.5.3]

4. Administration

According to the OAIS Reference Model Administration “provides the services and functions for the overall operation of the archive system. Administration functions include soliciting and negotiating submission agreements with Producers, auditing submissions to ensure that they meet archive standards, and maintaining configuration management of system hardware and software. It also provides system engineering functions to monitor and improve archive operations, and to inventory, report on, and migrate/update the contents of the archive. It is also responsible for establishing and maintaining archive standards and policies, providing customer support, and activating stored requests.”

4.1 Protection from Loss or Corruption

4.1.1 Disaster Preparation

4.1.1.1 An *Institution* SHOULD create backup and failure mode procedures for its records and vital records.  
[Indiana 1.9, 1.9.4; Pitt 2d; MoReq 4.3.7; InterPARES A.3; ISO 8.3.3]

4.1.1.2 An *Institution* SHOULD test and review backup and failure mode procedures.
4.1.2 Access Control

4.1.2.1 An *Institution* MUST explicitly assign responsibility for the annotation, relocation, and destruction of records on the basis of a person’s authority and capacity to carry out the activity (establishing user security profiles).

[Indiana 1.7.2, IP A.2, MoReq 4.6.5, 9.3.5; PRO A.5.36; ISO 9.7; PERM 25; HIPPA 45CFR 164.308(a)(3)(i), 45CFR 164.312(a)(1); Yale A.5]

4.1.2.2 An *Application* MUST confer exclusive capabilities upon people to exercise the responsibility for annotation, relocation, and destruction of records as defined by an institution.

[Indiana 1.4.1; DoD c2.2.5.2, c2.2.7.4; ISO 8.3.6; HIPPA 45CFR164.308(a)(1)(ii)(A); IP A.2]

4.1.2.3 An *Application* SHOULD manage the security level of the records it maintains, establishing records security profiles.

[MoReq 9.3.3, 9.3.5; PRO A.5.3.6]

4.1.2.4 An *Application* MUST NOT allow unauthorized changes to the records it maintains.

[Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.41; DoD c2.2.5.4; ISO 9.7.d; Yale A.4, A.7]

4.1.2.5 An *Institution* SHOULD create and maintain policies and procedures to detect, contain, and correct security violations.


4.1.2.6 An *Institution* SHOULD perform a periodic review of its security procedures.

[InterPARES B.1.b; HIPPA 45CFR164.308(a)(8)]

4.1.2.7 *Procedures* SHOULD allow for the periodic review of access control rules, records security profiles, and user security profiles.

[MoReq 4.6.12; PRO A.5.40; ISO 9.7; HIPPA 45CFR164.308(a)(3)(ii)(B)]
4.2 Reporting Capability & Event log

4.2.1 An Application MUST be able to identify system failures
[NARA 26.2.1]

4.2.2 An Application SHOULD be able to produce reports for administrators to
document any system activity, including failure.
[MoReq 3.4.14, NARA 26.2.4-26.2.6]

4.2.3 An Application MUST provide the capability to produce documentation of
any reproduction or copy process and its effects, including the dates of the
records’ reproduction and the name of the responsible person and the
impact of the reproduction process on the form of the records components
(any changes the records components have undergone).
[IP B.2]

4.2.4 An Application MAY provide the facility to isolate and resolve failures,
provided any activity is documented and any changes to affected records
components checked and documented.
[NARA 26.2.2-26.2.3]

4.3 System Administration

4.3.1 Procedures SHOULD contain provisions for all routine maintenance tasks
which fall in line with industry best practices.
[Pitt 2c; CTG System; NARA 26]

4.3.2 An Application MUST allow convenient access to and the ability to
modify any configuration parameters.
[MoReq 11.2.7, 9.1.1; NARA 26.4]

4.3.3 Infrastructure SHOULD provide the ability to monitor available storage
capacity.
[MoReq 9.14; PRO A.9.21; NARA 26.3]

4.3.4 An Institution SHOULD determine the acceptable ranges for downtime
and minimum numbers of simultaneous users.
[MoReq 11.3; DoD c3.1.3]
4.3.5  *Infrastructure* SHOULD be capable of fulfilling downtime and simultaneous user requirements laid out by the institution.  
[MoReq 11.3; NARA 26.4]

4.3.6  An *Application* MAY provide the capability to monitor overall system state in a consolidated manner.  
[NARA 26.3]

5.  **Preservation Planning**

According to the OAIS Reference Model Preservation Planning, “provides the services and functions for monitoring the environment of the OAIS and providing recommendations to ensure that the information stored in the OAIS remains accessible to the Designated User Community over the long term, even if the original computing environment becomes obsolete. Preservation Planning functions include evaluating the contents of the archive and periodically recommending archival information updates to migrate current archive holdings, developing recommendations for archive standards and policies, and monitoring changes in the technology environment and in the Designated Community’s service requirements and Knowledge Base. Preservation Planning also designs IP templates and provides design assistance and review to specialize these templates into SIPS and AIPs for specific submissions. Preservation Planning also develops detailed Migration plans, software prototypes and test plans to enable implementation of Administration migration goals.”

5.1  Preservation Planning framework

5.1.1  Develop Preservation Strategies

This subsection covers the process of establishing preservation strategies (sets of preservation action plans) for preserving records in a preservation system over time.

5.1.1.1  An *Institution* MUST establish plans for preserving records as long as needed.  
[Indiana 1.9; MoReq 11.7.4; PERM non dod 4; NARA 7.9]

5.1.1.2  An *Institution* SHOULD establish strategies for ensuring the accessibility and functionality of records components over time.  
[InterPARES A.4; ISO 8.3.5, 9.6]

5.1.1.3  An *Institution* SHOULD establish preservation action plans specifying preservation actions to be taken in ensuring the accessibility and functionality of templates of records components over time.  
[InterPARES A.4; ISO 8.3.5, 9.6; NARA 7.9]
5.1.1.4 An *Institution* SHOULD establish plans for managing preservation metadata and attaching it to records.

[MoReq 5.3.10, 11.7.7; PERM 5, 6]

5.1.1.5 An *Application* MAY provide the capability for users to create and maintain preservation and access plans

[NARA 7.9.1-7.9.4]

5.1.1.6 An *Application* MAY provide the capability for users to associate a preservation and access plan with electronic records

[NARA 7.9.5]

5.2 Monitor technology

5.2.1 Preserving *People* SHOULD monitor the state of the art of information technology in order to facilitate preservation planning.

5.3 Manage records templates

This subsection describes the management of records templates, sets of specifications about records. Every set of record stored in the system should conform to a template registered for that type of set of records, either at the time it is ingested into the system or through a subsequent transformation.

5.3.1 An *Institution* SHOULD define records templates to automate preservation planning and processing.

[NARA 6]

5.3.2 An *Application* MAY provide for management of templates within a template repository.

[NARA 6.1-6.7]

5.3.3 An Application MAY provide the capability to associate templates with sets of records.

[NARA 6.8.1-6.8.3]

6. Access

According to the OAIS Reference Model Access, “provides the services and functions that support Consumers in determining the existence, description, location and availability of information stored in the OAIS, and allowing Consumers to request and receive information products. Access functions include communicating with Consumers to receive requests, applying controls to limit access to specially protected information, coordinating the execution of requests to successful completion, generating responses (Dissemination
Information Packages, result sets, reports) and delivering the responses to Consumers.”

6.1 Use Rights
This subsection covers the institution’s management of users’ rights to view and/or receive records. This includes the development, management, and review of records and user security profiles. It also includes the management of access controls and authentication of users.

6.1.1 Access Controls
This subsection covers the management of processes that control the access of records in a preservation system.

6.1.1.1 Procedures MUST ensure that only authorized users gain access to records.
[MoReq 4.1.1; PRO A.5.25, A.5.42, A.5.46-50]

6.1.2 Record Security Profile

6.1.2.1 An Application MUST allow records security profiles to be created and modified.
[MoReq 9.3.5; PRO A.5.36]

6.1.2.2 An Application MUST allow record security profiles to be assigned to records.
[MoReq 4.6.1; PRO A.2.26, A.5.5, A.5.26, A.5.27; ISO 9.7.2]

6.1.2.3 An Application SHOULD allow time sensitive records profiles that are valid for a limited time period to be assigned to records and should automatically be switched to another records security profile when their valid time period expires.
[PRO A.5.38-39]

6.1.3 User Security Profile

6.1.3.1 An Application MUST allow user security profiles to be created and modified.
[MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]

6.1.3.2 An Application MUST assign or reassign user security profiles to people.
[MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]
6.1.4 Authentication of Users

6.1.4.1 *Infrastructure* SHOULD provide services for secure authentication.

[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPPA 45CFR164.312(d)]

6.1.4.2 An *Application* MUST authenticate users before providing services.

[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPPA 45CFR164.312(d); Yale A.4]

6.1.5 Access Review

6.2 Discovery and Delivery

6.2.1 Searching

6.2.1.1 An *Application* MUST ensure all of its records and metadata are discoverable.

[Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18]

6.2.1.2 An *Application* MUST be able to render all records returned in a search results list.

[MoReq 8.2.1; PRO A.3.20; DoD c2.2.6.8.10]

6.2.1.3 An *Application* MUST support searching by records’ identifiers.

[MoReq 8.1.16, 8.1.23]

6.2.1.4 An *Application* SHOULD provide an integrated search interface.

[MoReq 8.1.2; PRO A.3.7]

6.2.1.5 An *Application* MUST, if it has an integrated search interface, present search results.

[PRO A.3.15; DoD c2.2.6.8.5]

6.2.1.6 An *Application* SHOULD support external search engines in addition to any integrated search interface.

[PRO A.3.19]

6.2.1.7 An *Application* SHOULD limit search results to the records the user has rights to access.
6.2.1.8 An Application MAY provide capabilities to manage a search results list including, but not limited to, order, number of hits per page, filter results files, and saving search results.

[MoReq 8.1.17; 8.1.24-25; DoD c2.2.6.8.5]

6.2.2 Query Techniques

6.2.2.1 An Application SHOULD support the full text search of the records and metadata it maintains.

[MoReq 8.1.8; DoD c3.2.9]

6.2.2.2 An Application SHOULD support searching metadata fields containing controlled vocabulary terms managed by thesauri.

[MoReq 8.1.10; PRO A.3.5; DoD c3.2.9]

6.2.2.3 An Application SHOULD support searching multiple metadata fields and/or full text of records.

[MoReq 8.1.6; PRO A.3.9; DoD c2.2.6.8.2]

6.2.2.4 An Application SHOULD support the use of Boolean and/or relational search operators such as “and” “or” “not” “less than” “greater than” “equal to.”

[MoReq 9.1.8; PRO A.3.13; DoD c2.2.6.8.4]

6.2.2.5 An Application SHOULD support wild card and/or pattern matching searches.

[MoReq 8.1.11; PRO A.3.13; DoD c2.2.6.8.3]

6.2.2.6 An Application SHOULD support the iterative refinement of a search by adding search conditions to a previously run search—i.e. narrow a search.

[MoReq 8.1.21]

6.2.2.7 An Application MAY support word proximity searching.

[MoReq 8.1.12]

6.2.2.8 An Application MAY support searching null values.

[DoD c2.2.6.8.6]

6.2.2.9 An Application MAY support searching time intervals.

[MoReq 8.1.22]
6.2.3 Rendering Complex Objects

6.2.3.1 *An Application* MUST render all of the components of a record and its metadata in a logical manner.

[Indiana 1.10.4; MoReq 8.2.3; PRO A.3.21]

6.2.3.2 *An Application* MUST be able to render records together with their associated metadata.

[MoReq 8.1.15; PRO A.3.24; DoD c2.2.3.21; PERM 23]

6.2.3.3 *An Application* MUST be able to render records on to appropriate output media, which should at least include graphical display and printer output.

[MoReq 8.2, 8.3, 8.4.1; Pro A.3.25-26, A.3.28-29; PERM 3, 10, 14, 16, 17, 24, non dod 2]

6.2.3.4 *An Application* SHOULD be able to render records into an open export format.

[PRO A.3.31]

6.2.3.5 *An Application* SHOULD be able to render records independently of their creating environments.

[MoReq 8.2.2; PRO A.3.22; DoD c3.2.14]

6.2.3.6 *An Application* SHOULD be able to render a record simultaneously for multiple users.

[PRO A.3.23, DoD c2.2.7.5]

6.2.3.7 *An Application* SHOULD be able to render all versions of a record.

[DoD c2.2.6.8.9]

6.2.4 Rendering Recordness

6.2.4.1 *An Application* MUST render a record’s content.

[Pitt 11, 12; MoReq 8.2.3; PRO A.3.21; PERM 2]

6.2.4.2 *An Application* MUST render a record’s structure.

[Pitt 12, 12b, 12b1; PRO A.3.21; PERM 2]

6.2.4.3 *An Application* MUST render a record’s context.

[Pitt 12, 12b1, 12c; ISO 7.25; PERM 2]
6.2.4.4 An Application MUST render a record’s functionality.
[Pitt 11b, DoD c2.2.5.3]

6.2.5 Redaction

6.2.5.1 Procedures SHOULD provide for the redaction of restricted content from records delivered to users that do not have the right to see the restricted output.
[Pitt 13, MoReq 9.3.10; PRO A.2.56]

6.2.5.2 An Application SHOULD be able to create redacted versions of textual, audio, and moving image records.
[MoReq 9.3.10]

6.2.5.3 An Application MUST NOT, if it can redact records, alter the content of a record while creating a redacted version of that record.
[Pitt 13a; PRO A.2.56]
V. Degrees of Obligation for each Requirement

In this document each records preservation requirement is qualified by one of five modal auxiliary verbs used to express different degrees of obligation. These different verbs are: MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY. To ensure clarity and accuracy, this document adheres to the RFC 2119 standard for defining requirement levels.¹ It is important to understand the precise meanings of each of these keywords, particularly because each does not necessarily represent the most commonly accepted meaning of the word. The use of each keyword is described below:

MUST. This word means that the definition is mandatory, or an absolute requirement of this specification. If this requirement is not fulfilled, the system cannot be considered to be a trustworthy records preservation system.

MUST NOT. This phrase means that the definition is an absolute prohibition of the specification.

SHOULD. This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. Such a requirement is highly desirable. If the requirement is not fulfilled, the level of trust in the records preservation system will be diminished.

SHOULD NOT. This phrase mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY. This word means that an item may be desirable, but truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation that does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality. In the same vein an implementation that does include a particular option MUST be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature the option provides.)

¹ Scott Bradner, RFC 2119: Key words for use in RFCs to Indicate Requirement Levels, Network Working Group <http://www.ietf.org/rfc/rfc2119.txt?number=2119>,