Functional Requirements for Electronic Records

Overview
This document represents a set of mandatory recordkeeping requirements for systems that capture and manage electronic records. Records in the context of this document are defined as “recorded information, in any form, including data in computer systems, created or received and maintained by an organization or person in the transaction of business or the conduct of affairs and kept as evidence of such activity.”

Recordkeeping systems in the context of this document are defined as "systems which capture, manage and provide access to records through time.” More specifically, recordkeeping systems include: 1) a set of authorized polices, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorize and promulgate the policies, procedures and practices; 2) the records themselves; 3) metadata and record classification systems used to control and manage the records; and 4) software, hardware and other equipment.” (National Archives of Australia, DIRKS, Glossary)

The requirements for recordkeeping outlined in this document are the “identified needs for evidence arising from various internal and/or external sources that may be satisfied through appropriate recordkeeping actions (such as creation, capture, maintenance, preservation and access). The sources include legislative and other regulatory sources, industry codes of best practice, broader government interests, external clients or stakeholders and the general public.” (National Archives of Australia, DIRKS, Glossary). A record that is automatically captured and managed by an ERMS can, in most cases, be considered to be authentic and trustworthy by meeting these requirements.

Requirements:

1.1 Compliance
The system must manage and control electronic records according to the standards for compliance and the requirements for legal admissibility and security and must be capable of demonstrating this compliance.

1.1.1 The system must meet legal requirements as set forth by local, state, and federal statutes and regulations.

1.1.2 The system must meet administrative requirements.
1.1.3 The system must meet federal and international standards.

The standards will vary from system to system. For applicable standards, consult the websites and publications for the following organizations:

- International Organization for Standardization (ISO) ~ http://www.iso.ch
- National Information Standards Organization (NISO) ~ http://www.niso.org/
- American National Standards Institute (ANSI) ~ http://www.ansi.org/
- AIIM International ~ http://www.aiim.org/

1.1.4 The system must meet all "best practice" guidelines.

Many national organizations have developed guidelines for their specialty areas. These guidelines represent requirements that are generally accepted practices or industry standards.

1.2 Record Capture

The term capture represents the processes of registering a record, deciding which class it should be classified to, adding further metadata to it, and storing it in the ERMS.

It is recommended that, whenever possible, the capture function be designed into electronic systems so that the capture of records is concurrent with the automatic creation of records.

1.2.1 The system must capture a record for all defined functions and activities.

Records may be captured within a system manually or by automatically by the system itself either as part of the system's workflow or through a batch process. The type of business processes should determine the exact method of creation.

1.2.2 The system should capture records through an automated process.

Ideally, the capture of records would occur automatically without human intervention. This could be done utilizing a business process or a workflow engine.

1.2.3 The system must capture all metadata elements specified during the system design process and retain them with the record in a tightly bound relationship.
1.2.4 The system must ensure that records are associated with a classification scheme and are associated with one or more electronic files.

Electronic files can be defined simply as a set of electronic records. A file is a group of records accumulated and kept together because they deal with the same subject, activity or transaction. In other words, there is some common bond or relationship between records in a file. Electronic files need not have real existence; often they are virtual entities and exist because the metadata attributes of the records and the application software allows users to view and manage folders as if they physically contained the records assigned to them.

1.2.5 The system must register the record by assigning it a unique identifier and documenting the date and time when the record entered the recordkeeping system.

An identifier is an attribute that distinguishes individual instances of a record or file within a system. It is recommended that the identifier be a number or alphanumeric sequence that is automatically and randomly generated.

1.2.6 The system must maintain a logical relationship between the record and the transaction it documents.

1.2.7 The system must allow a compound document to be captured as a single record.

Some electronic records, such as web pages with graphics or e-mail messages with attachments, are composed of more than one component. The system must capture all of these components and maintain them as one record. This means maintaining the relationships between the components to ensure future retrieval, rendering, management, and retention or disposal.

or,

The system must allow a compound document to be captured as linked simple records.

In this strategy, each part of the compound record will be captured separately then linked to the other parts.

1.2.8 The system must support versioning.
Sometimes, records have more than one version that must be captured. The system must allow either the capture of all versions as one record or the capture of each version as separate records. In the later case, a version number should be added to the metadata.

1.2.9 The system must be capable of capturing transactional documents generated by other systems. In the case of large, centralized OLTP systems, the ERMS must allow for the bulk capture of records created or maintained in these systems.

Transactional records such as invoices or purchase orders can often be captured as batch file imports from other systems. The system must allow for this bulk transfer and must provide methods for ensuring data integrity and the capture of all essential metadata.

1.2.10 The system must be able to capture a variety of different types of documents. These must include records from on-line transaction processing systems (OLTP), databases, scanned documents, the most commonly used office documents, and e-mail messages.

In some cases, it would be impractical for a system to capture all document types. Before building a system, management should decide the document types that must be captured.

1.2.11 The system must be integrated with the e-mail system, and e-mail must be captured and registered either by requiring that users capture selected e-mail and/or by providing an automated process for capturing the e-mail messages.

1.2.12 The system must ensure the reliability of the capture process.

To make a system like this work, the capture process must be reliable as records are migrated from the creating system or storage medium to the ERMS. Records cannot be lost or changed during the capture process.

1.3 Classification Scheme

Classification is the systematic identification and arrangement of records into categories according to logically structured conventions, methods, and procedural rules represented in a classification scheme. The classification scheme, sometimes also called a file plan, is a diagram, table, or other representation categorizing the creator's records, usually by hierarchical classes, and according to a coding system expressed in alphabetical, numerical, or alphanumerical symbols. The benefits of a good classification scheme are “1) providing linkages between individual records; 2) ensuring records are named in a consistent manner over time; 3) assisting in the retrieval of all records
related to a particular activity; 4) determining appropriate retention periods for records; 5) determining security protection appropriate for sets of records; 6) allocating user permissions for access to or action on particular groups of records; and 7) distributing responsibility for management of particular sets of records." (“TRIM and AS 4390 Records Management Standard”).

There are many types of classification schemes, but the one recommended by this document is a scheme based an articulation of the functions and transactions of the organization derived from the analysis of business processes. The business classification scheme represents and describes functions, business processes, transactions or other elements, and shows their relationships. The number of levels within the scheme can vary depending on the level of refinement required and how the scheme will be used. The structure of the scheme is hierarchical, moving from the general to the specific. Each function has business processes and each process (linked to the function) has categories of transactions that are encountered. “In other words, a classification scheme based on a rigorous classification of business processes means that records are classified on the basis of why they exist (their function or the business event that caused the record to be brought into existence), rather than on the basis of what they are about (their subject). As such, the focus of classification is the context of a record’s creation and use, rather than the content of the record itself.” (National Archives of Australia, DIRKS, Glossary)

A thesaurus often supports classification schemes. “A thesaurus is a complex alphabetical listing of all terms derived from a classification scheme. Such tools act as a guide in the allocation of classification terms to individual records. In a thesaurus the meaning of the term is specified and hierarchical relationships to other terms are shown. A thesaurus should provide sufficient entry points to allow users to navigate from terms which are not to be used to the preferred terminology adopted by the organization.” (National Archives of Australia, DIRKS, Glossary). In particular, it is important to create a function thesaurus, which contains keywords, descriptors and forbidden terms that describe the unique business functions and processes of an organization.

1.3.1 The system must support and be compatible with the organization’s or the application’s classification scheme.

When the classification scheme is non-existent or only partially constructed, or when designing a new system, it is strongly recommended that the classification scheme be based upon business processes and the identification of the business transactions that create records.

1.3.2 The system must automatically assign appropriate classification metadata to records and files and to classes within the classification scheme at the point of creation and capture.
1.3.3 The system must ensure that the authorization to reclassify, add, delete or otherwise modify the classification scheme is carefully controlled and monitored.

1.4 Authenticity

To be authentic in archives and records management, a record must be genuine, or be “what it claims to be.” Authenticity is conferred to a record by its mode, form, and/or state of transmission, and/or manner of preservation and custody. (University of British Columbia Electronic Records Project). In order to trust that a record is authentic, the user must be assured that the systems that create, capture, and manage electronic records maintain inviolate records that are protected from accidental or unauthorized alteration and from deletion while the record still has value. The following requirements must be met to ensure that a record's integrity can be proven.

1.4.1 The system must maintain secure and inviolate records, including record content and metadata that documents content, context and structure.

Preserving an inviolate record and all record components is vital for proving the authenticity of records. To ensure that records are protected, the system must control access to its records and log access through audit trail functionality (discussed in Section 15.). In some cases, a record may be modified as part of a business process. Modifications of this type may be handled through version control, or a department of organization may elect to transfer the record to an ERMS until it is complete.

1.4.2 The system must ensure that records cannot be deleted by any means except as directed by a retention schedule.

1.4.3 The system must undergo regular and systematic audits to verify system integrity.

Software bugs and insecure access points, along with other problems, can destroy the authenticity of the records a system contains. Regular system audits can help prevent these problems.

1.5 Audit Trails

A system audit trail is a record that tracks operations performed on the system and documents the activities performed on records and their metadata from creation to disposal. These activities may be initiated by users, system administrators, or by the system itself by means of automatic processes. The audit trail typically documents the activities of creation, migration and other preservation activities, transfers or the movement of records, modification, deletion, defining access, and usage history. By
maintaining evidence of activities undertaken on records and files, a detailed audit trail is critical for ensuring that a system meets all basic requirements for a viable records management environment.

1.5.1 The system must maintain audit trails for all processes that create, update or modify, delete, access and use records, categories or files of records, metadata associated with records, and the classification schemes that manage the records.

*These processes include, but are not limited to, creation, import or export process, modifications, transfer, destruction, deletion, access and use of a record, electronic files, metadata, classification schemes, and disposition schedules.*

*At a minimum, it tracks:*  
- what data or information was accessed, added, deleted or modified;  
- who performed these functions; and  
- when they were performed.

1.5.2 The system must automatically capture the audit trail.

*The system must track events without manual intervention, and automatically stores information about these activities in the audit trail.*

1.5.3 The audit trail data must be unalterable.

*The system must ensure that audit trail data cannot be modified in any way.*

1.5.4 The audit trail must be maintained for as long as required by law or policy or to facilitate continued access to records.

*At a minimum, the audit trail must be kept until the records it refers to are destroyed. Even after record content is destroyed, however, some audit data should be retained relating to the retention and destruction of the record.*

1.5.5 The audit trail must be logically linked to the records they document, so that users can review audit information when they retrieve records.

*This logical relationship must be maintained even when the records and audit are stored in different systems.*
1.5.6 The audit data must be available for inspection or export (without affecting vital audit trail data) by authorized users with little or no experience with the system. This requirement is necessary to enable users such as internal or external auditors to investigate system activity.

1.5.7 The system must maintain basic system documentation and audit trails of system modifications as long as they are required to facilitate continued access to records. This includes tracking all changes made to system hardware or software and to administrative parameters such as changing user access rights.

1.5.8 The system must provide reports for actions taken on basis of audit trail data. The department or organization will determine what audit trail reports are needed and how they are organized. Possible reports include, but are not limited to, a chronological listing of activities for the entire system; a listing of activities involving an individual record, file, or class; a listing activities taken by a particular user; and a listing of activities taken at a particular workstation.

Implementation Note: Since the volume will be quite large, on-line audit trail data may periodically be moved to off-line storage. Also, some audit trail data may be deleted once the records referred to are destroyed according to an approved retention schedule. In some cases, management may decide that some activities do not need to be recorded. Notations about all of these issues and their results must be kept with the system documentation or within the audit trail itself.

1.6 Metadata

In the context of archives and records management, metadata is structured or semi-structured information that documents the creation, management and use of records through time and across domains. Recordkeeping metadata can identify, authenticate and contextualize records and the people, processes and systems that create, manage and use them.

1.6.1 The system must be capable of extracting metadata elements automatically from records when they are captured.
1.6.2 The system must permit metadata values to be retrieved and captured from lookup tables or from calls to other software applications.

1.6.3 The system must allow creators of records to enter manually pertinent record metadata that cannot be captured automatically.

1.6.4 The system must support the validation of metadata that is entered by users, or metadata that is imported from other systems.

1.6.5 Metadata must be logically linked to the records, files, and classes it documents, so that users can review metadata information when they retrieve records.

1.6.6 The system must allow for the modification or reconfiguration of metadata sets, but the authorization to make changes must be restricted.

1.7 Security and Control
The system must include quality control mechanisms to ensure that consistent and accurate business records are created.

1.7.1 The system must allow only authorized personnel to create, capture, update or purge records, metadata associated with records, files of records, classes in classification schemes, and retention schedules.

1.7.2 The system must control access to the records according to well-defined criteria.
   
   A user must never be presented with information that he or she is not permitted to receive. The criteria for access will vary according to the type of data or records contained in the system.

1.8 Retention and Disposition
The system must include an automated, schedule-driven disposition management plan.

1.8.1 The system must provide for the automated retention of records with long-term value in accordance with authorized and approved record retention schedules.

1.8.2 The system must provide for the automated destruction of records in accordance with authorized and approved records retention schedules.
1.8.3 The system must be capable of associating a retention schedule with all records, record metadata, files or classes of a classification scheme.

1.8.4 The system must automatically provide for the notification and approval of designated personnel in advance of disposition activities.

1.8.5 The system must provide for the interruption of disposition activities on records or classes of records that have been or are expected to become the subjects of litigation.

1.8.6 Within the system, every record in a file or class of records must be governed by the retention schedule associated with that file or class.

1.8.7 The system must allow the administrator in charge of schedules to change or amend schedules associated with records at any point in the life of the record.

1.9 Preservation Strategies, Backups and Recovery

The system must incorporate a strategy or plan for backing up and preserving records.

1.9.1 The system must ensure that records, components of records, audit trails, metadata, links to metadata or to files, and classification schemes can be converted or migrated to new system hardware, software and storage media without loss of vital information.

1.9.2 The system must produce a report detailing any failure during a conversion or transfer and identifying records that were not successfully exported.

1.9.3 The system must retain all records that have been exported until confirmation of a successful transfer process.

1.9.4 The system must provide automated procedures that allow for the regular backup and recovery of all records, files, metadata, and classification schemes.

*Backup procedures must not be regarded as substitute for a preservation strategy based on procedures for conversion or migration of records on a regular schedule.*
1.10 Access and Use

The system must ensure access to and use of business records for current business and future research needs.

1.10.1 The system must ensure that records can be easily accessed and retrieved in a timely manner in the normal course of all business processes or for reference or secondary uses.

1.10.2 The system must allow all record content and all record and file metadata to be searchable.

1.10.3 The system must allow searching within an electronic file, across files, at any level in the classification scheme hierarchy.

1.10.4 The system must ensure that all components of a record or file, including contents, relevant metadata, notes, attachments, etc., can be accessed, retrieved and rendered as a discrete unit or group and in a single retrieval process.

1.11 Documentation

All system policies and procedures must be defined and documented. This documentation helps to ensure continuing access to records within the system, and can be used to help prove the authenticity of a record.

1.11.1 System administrators must maintain policy and procedural documentation.

    The documentation should include at a minimum an overview of the purpose and uses of the system; policies and procedures for system operation and maintenance, quality control, security, testing, and records retention; and software/hardware specifications and operation.

1.11.2 Documentation must be accurate and up-to-date.

1.11.3 Documentation must be written clearly and concisely.

1.11.4 Documentation must readily available and accessible.

1.11.5 Documentation must be retained according to an approved retention and disposition schedule.

1.12 System Testing
1.12.1 The performance and reliability of system hardware and software must be regularly tested. The exact nature of the tests will depend on what is appropriate for that particular hardware and software and will be defined by system support personnel in conjunction with EITS.

1.13 Non-Electronic Records
The system must be capable of classifying and managing non-electronic, physical records and of managing electronic and non-electronic records in an integrated manner. This means the system must be able to classify, create and retrieve audit information and other metadata, control access and define security, and apply retention and disposal schedules for non-electronic records according to the same requirements that have been defined for electronic records.