ELECTRONIC RECORDS MANAGEMENT
AND
ARCHIVES MANAGEMENT POLICY

Guidelines on Electronic Records Management: Managing Electronic Records in the Structured Environment

NATIONAL ARCHIVE OF MALAYSIA

ARKIB NEGARA MALAYSIA

Projek Pemeliharaan Rekod Elektronik Sektor Awam
(e-SPARK)

Project Documentation

***Guidelines on Electronic Records Management:
Managing Electronic Records
in the Structured Environment***

Managing Electronic Records in the Structured Environment

Preface

This Guideline was produced as a result of the e-Spark initiative. Sponsored by the Arkib Negara Malaysia and involving public offices and agencies from across the Government of Malaysia, the purpose of this initiative was to develop policies, standards and practices, technical specifications and training plans to enable the Government of Malaysia to manage records in electronic form. Also included was a strategic plan reflecting the roles and responsibilities of public offices and various central and lead agencies. The Arkib Negara Malaysia, within its legislative mandate to facilitate the management of records in any physical form and to acquire, preserve and make available those of archival value, is the lead public office responsible for facilitating the government-wide management of electronic records. In this capacity and in cooperation with other central agencies and government public offices it is responsible for issuing standards and guidance to government public offices on the management of electronic records.

Managing Electronic Records in the Structured Environment is one of a series of guidelines that have been developed to help government public offices and agencies manage electronic records. This guideline should be used in conjunction with the general guideline, *Guidelines on Electronic Records Management* (also available from the Arkib Negara Malaysia). Companion guides are: *Managing Electronic Records in the Unstructured Environment* and *Managing Electronic Records in the Web Environment.*

These guidelines should also be used in conjunction with *Electronic Records and the Akta Arkib Negara 2003* (available from the Arkib Negara Malaysia). This publication supports the implementation of the Akta Arkib Negara 2003 and the requirement by government departments not to dispose of their records without the approval of the National Archivist and to transfer records assessed as having archival value to the control of the Arkib Negara Malaysia.

For additional information, please contact:

Arkib Negara Malaysia,
Jalan Duta,
50568 Kuala Lumpur
Tel. 603-62010688
Fax. 603-62015679
Web Site: http://arkib.gov.my

Table of Content

Managing Electronic Records in the Structured Environment

1. Purpose

The purpose of this Section is to provide Public offices with guidance on how electronic records can be managed in the structured environment. The guidance is designed for systems developers, database administrators, system support staff, records management staff and program managers responsible for business information systems. This guide should be used in conjunction with **Guidelines on Electronic Records Management** (available from the Arkib Negara Malaysia).

2. The Structured Environment

The **structured environment** is an environment where business processes are typically highly structured, well-established tools and techniques are employed to develop application systems supporting the processes, and accountability for the design, development and maintenance of systems (including the integrity of the data generated in the systems) has been assigned. This is the 'business information systems' world where the processes for carrying out the business of the organization have been heavily structured, where accountability for the design, development and maintenance of the systems supporting these processes has been assigned and where the accuracy and reliability of the 'data' generated and managed in these systems must be ensured in order to support the overall integrity of the systems.

Business information systems are designed to support a specific business process – for example, case management systems, geospatial data systems, finance or human resource systems, call centre systems or systems that support e-business and online transactions. They are usually transaction-based systems. As such, they rely heavily on system logs (e.g. audit trails) to track changes to data and attempts to access their contents.

The management of records should work best in this kind of environment because a platform of accountability, defined work processes and business rules and a codified approach to systems and data design has been established. It doesn't always succeed (which is why there are records issues – most notably in establishing records authenticity and addressing retention, disposition and long-term preservation) but at least a framework of policies, standards and practices, systems and technologies and people exists to manage the processes and the multiple forms of information generated by the processes. Usually, in the absence of an adequate understanding of record keeping issues in this environment, the solutions tend to be derived from the world of systems development and data management.

3. Electronic Records Issues

The guidance in this Section focuses on the three important aspects of electronic records management that present special challenges with respect to the design, development, implementation, and review of business information systems. These are as follows:

Establishment of records authenticity. That is, how to ensure that the elements of a complete and accurate record of an action or transaction can be rendered as required for as long as required in order to serve as an 'authentic' record of the action or transaction.

Establishment and application of records retention and disposal specifications. That is, how to set retention specifications for electronic records in complex systems and how to dispose of records either through deletion or transfer to the Arkib Negara Malaysia as archival records

> Example: How to set a retention period for the completed electronic application forms that is within the context of the retention periods set for all of the other records generated by the business process supporting the licensing function?

> Example: How to ensure that the completed electronic application form for a new license is an authentic record of the action invoked by an individual to apply for a license.

Preservation of electronic records for as long as required. That is, how to ensure that the integrity and reliability of the record can be maintained through a given period of time?

> Example: How to preserve the completed electronic application forms over the long term (as perhaps required by law) in spite of changes to the technology environment in which they were originally created?

4. Managing Electronic Records in the Structured Environment[1]

The guidance that follows is designed to address these aspects. It is based on the assumption that generally accepted systems development methodologies already contain the framework for ensuring that these issues are addressed (i.e. it is a natural part of the systems development life cycle). It is also based on the assumption that:

---

[1] The guidance in this section was based on similar guidance developed for the Government of Hong Kong by the Government Records Service, 2002

- Business information systems have the capability to meet the 'Conditions for Capture, Maintenance, and Use' of records as described in Appendix 1.
- Designated officials within the public office have been assigned accountability for the integrity of the business information systems.
- The development of new business information systems and the enhancement or redesign of existing systems are based on a generally accepted systems development life cycle (SDLC) – the system is planned, designed, implemented and reviewed according to a structured set of pre-defined steps.

The guidance is also based on government policy that requires public offices to capture and maintain complete and proper records of their programs and activities in order to satisfy business and accountability needs. In this connection, records must be accurate, reliable and authentic so that they can support daily business activities, serve as evidence of decisions and activities and provide for the accountability of government administration.

To meet the recordkeeping needs, the following basic measures are recommended for records generated in the structured environment:

- Maintain written policies and procedures which define the records and related metadata, the ways in which they must be managed and the operations for development, maintenance and use of such records, their application systems and the recordkeeping system.
- Provide sufficient training and support to staff to help ensure that the above policies and procedures are understood and implemented.
- Build recordkeeping requirements into the application systems to make sure that records are captured and maintained in a recordkeeping system.
- In consultation with the Arkib Negara Malaysia, draw up records retention and disposal schedules
- Develop system controls to ensure the accuracy and reliability of the records generated in application systems.
- Implement system audit trails to record the history of the creation and use of the records in the application systems. Through the audit trails, public offices should be able to track who had access to the system, whether staff followed certain procedures and whether fraud or unauthorised activities occurred, etc.
- Conduct routine and regular performance tests on the application systems, including hardware and software, so that system reliability and information integrity can be guaranteed.
- Provide adequate security to limit access and update privileges to authorized personnel.
- Maintain comprehensive documentation in respect of system design, implementation, operation and maintenance, such as software requirement documentation, documentation about the system architecture, hardware/software maintenance procedures, data definition and user documentation.
- Dispose of the records and related documentation according to the records retention and disposal schedule agreed by the Arkib Negara Malaysia and document the disposal actions taken.

- Develop long-term retention and migration strategies, where necessary, to make sure that the electronic records can be maintained and used for as long as required.

There are two categories of systems to which this guidance applies: **new application systems** and **existing application systems.**

Public offices should follow the guidance provided below when major enhancements/upgrades for existing mission-critical systems and new mission-critical systems are introduced. In ascertaining the need to assess (and to implement, as required) recordkeeping requirements for both categories of system, public offices should consider the following:

- The importance of the electronic information in the systems to their legal, fiscal, operational and accountability requirements.
- The extent to which the systems are 'mission-critical'. Mission-critical systems refer to those application systems performing or supporting business functions or activities that are essential to the primary missions of public offices.
- The adequacy of existing recordkeeping measures and procedures.
- The costs and consequences (i.e. level of risk) associated with implementing and not implementing the recordkeeping requirements.

4.1 New Systems or Existing Systems about to be Re-designed

The following procedures should be followed for new systems or systems that are to be redesigned. Within this context, emphasis should be given to mission-critical systems. The procedures have been organized according to the generic stages of the systems development life cycle and as such are suitable for adaptation by individual public offices for incorporation in their systems development methodologies.

Planning

Measures to be taken are as follows:
- Determine at what point a transaction within the business process supported by the planned application system will be creating a record.
- Define the structural and contextual attributes of the record that the system needs to capture.
- Determine the rules for how records should be captured when performing a transaction.
- Identify relevant laws, regulations, policies and standards.
- Incorporate the recordkeeping requirements identified in laws, policies, regulations and standards (including records retention and disposal requirements) into the functional requirements, data architectures, data models, etc. for the application system.

- Identify security features that need to be included, such as the ability to restrict access to systems functions and records to appropriate staff or to secure the transmission of electronic records.
- Ensure that appropriate audit trails are created that will reflect accurately the history of the record's creation, use, and retention.
- Ensure that any related paper records (e.g. hard copies of system inputs and outputs for entering, updating and deleting data and producing reports, etc.) are accounted for.
- Assign responsibility (within the accountability framework for the overall application system) for ensuring that records are generated and captured and that their authenticity and integrity are managed through their life cycle.

Project initiation

Measures to be taken are as follows:
- Establish an agreement, project charter, etc. (within the context of project charters established for the planned application system) that cover the steps involved in describing the system for ensuring that the records' authenticity can be maintained through time, setting retention specifications for records in the system and establishing records disposal schedules, etc.
- Establish a governance structure (within the context of the governance structure for the planned application system) that ensures the collaboration of key individuals such as the application system manager, programme manager, systems developers, records managers, registry staff, etc.

Requirements definition

Measures to be taken are as follows:
- Within the context of the functional requirements for the planned system, ensure that requirements for the setting of retention specifications, authenticity requirements, disposal scheduling, potential migration strategies, etc. are accounted for.
- Develop procedures and rules for how the retention and disposal specifications should be carried out (i.e. who is responsible for applying the retention specifications to the electronic and related paper records; who is responsible for and how are records disposed of; etc.).
- Identify requirements for training and change management to ensure that those administering the recordkeeping aspects of the application system are able to respond to the functional requirements and the rules and procedures.
- Undertake capacity planning checks to identify the volume of the electronic records to be retained and identify the facilities required to manage such records according to the prescribed retention specifications (i.e. for both paper and related electronic records).
- Identify requirements for the disposal of electronic records to ensure that they are disposed of according to the specifications incorporated in the design of the planned application system and in accordance with retention and disposal schedules approved by the Arkib Negara Malaysia; and

- Identify a funding strategy for addressing the recordkeeping issues and incorporate into the funding strategy employed for the planned application system.

Design

Measures to be taken are as follows:
- Incorporate the recordkeeping requirements into the relevant data and systems architectures for the planned system.
- Ensure that the proposed requirements can be accommodated within the existing or planned technology infrastructure supporting the planned application system.
- Establish performance measures for the recordkeeping requirements within the context of the performance measures established for the planned application system.

Implementation and Review

Measures to be taken are as follows:
- Confirm that the recordkeeping requirements have been accounted for during the actual development or modification of the application system.
- Undertake awareness and training concerning the recordkeeping aspects of the new or redesigned application system within the context of the overall awareness and training strategies established for the system.
- Ensure that the policies, standards and practices, and technology architecture account for the recordkeeping requirements.
- Undertake user acceptance tests of the recordkeeping capabilities of the system within the context of the acceptance tests conducted for the new or modified system.

4.2 Existing systems

To help develop appropriate strategies and practices for existing application systems, Public offices should categorize their systems in terms of data permanence (**'static'** or **'dynamic'**[2]) and system life time (**'open'** or **'closed'**[3]) as follows:

'Static closed system' – an application system in which data are never removed or overwritten after creation and new data will not be inputted.
'Static open system' – an application system in which data are never removed or overwritten after creation and new data will be inputted.
'Dynamic closed system' – an application system in which old data are overwritten by new data and new data will not be inputted.
'Dynamic open system' – an application system in which old data are overwritten by new data and new data will be inputted.
'Combined system' – an application system where both dynamic and static data are found.

---

[2] Data in a 'static system' are never removed or overwritten after creation while those of 'dynamic system' will be replaced by new data as/when required after creation.
[3] 'Open system' is an application system that is still in operation while 'closed system' refers to a defunct application system.

4.2.1 Existing Systems: Issues

Authenticity

In the case of existing systems, the challenges facing Public offices with respect to electronic records are as follows:

- The records and the recordkeeping system may lack sufficient metadata to relate the record to its context of creation and use.
- The record may lack information (e.g. audit trails, digital signatures, etc.) to confirm authorship;
- The record may be managed in a system that lacks the attributes required to ensure the record's authenticity through time. These attributes can include:
    - o Audit and security features for ensuring the integrity of the system;
    - o Access controls for controlling unwarranted access to the records; and
    - o Personnel accountable for maintaining the integrity of the system and the authenticity of the records over time.
- The records and the recordkeeping do not meet the conditions described in Appendix 1.

To ensure the authenticity of records in **'closed systems'** (i.e. 'static closed systems' and 'dynamic closed systems'), public offices should take the following measures:

- In consultation with Arkib Negara Malaysia, develop a records retention and disposal schedule and prescribe the retention and disposal requirements for the records in the application system.
- Check the design of the application system against the conditions set out in Appendix 1 for compliance.
- Provide documentation to make sure that the date when the application system was closed is documented and the contextual information explaining what the records contain, why they were created and how they were managed through time is available and complete.
- Examine the effectiveness of the system security measures to see if the records have been tampered with since the application system was closed.
- Evaluate the need to enhance or redesign the system if the data are still required for use. If such a needs exists, follow the guidance in this Section to redesign the system[4].
- Dispose of records and related documentation according to the records retention and disposal schedule agreed by the Arkib Negara Malaysia.

For records in **'open systems'** (i.e. 'static open system' and 'dynamic open system'), in addition to the guidance provided for 'closed systems', public offices should:

- Confirm that accountability for the integrity of the application system and the records generated in the application system have been assigned to appropriate personnel (such as system administrator, program manager and records manager). This is to ensure that:
    - o The application system is able to manage records as authentic records.

---

[4] It should be noted that in most cases, 'closed system' in public offices will not be redeveloped unless the records are very important to the current operation of public offices and/or they have continuous or long-term retention value.

- The records generated in the application system reflect attributes of authenticity such as the availability of sufficient metadata, the existence of signatures (where necessary) or audit trails to confirm authorship, and the comprehensive and effective combination of the content, structure, and context required to document actions and activities.
- Develop system audit policy and procedures and conduct audits on a regular basis to evaluate the extent to which the records can serve as authentic records of the actions and transactions they are documenting.
- Evaluate the need to redesign the system to make sure the above are fulfilled. If required, follow the guidance in this Section to ensure that recordkeeping requirements are reflected in the redesigned system.

Retention and disposal

The common problems in the area of records retention and disposal for existing systems are summarized as follows:
- Retention periods do not conform to the regulatory requirements and business needs of the public office.
- Retention periods for electronic records are not consistent with those for related paper records generated in the same system.
- Retention and disposal practices are not covered by records retention and disposal schedules issued by the Arkib Negara Malaysia.
- Accountability has not been assigned to appropriate personnel for ensuring that retention and disposal specifications are incorporated in the design of the system and the retention and disposal procedures are reviewed periodically.

Measures to be taken for records in **'closed systems'** (i.e. 'static closed systems' and 'dynamic closed systems') are as follows:
- In consultation with the Arkib Negara Malaysia, identify how long each database is to be retained based on operational, legal, fiscal and archival requirements and set the retention period at the level of the database, as far as practicable[5];
- Ensure that related system documentation and paper records are also accounted for in the retention and disposal schedule;
- Link the database to the appropriate area of the public offices' records classification system based on cross references in the classification system and in the retention and disposal schedules completed for the database; and
- Retain and dispose of the database and related system documentation and paper records in accordance with the records retention and disposal schedule agreed by the Arkib Negara Malaysia.

Depending on the extent of data permanence in an 'open' system, records in the 'static open systems' and 'dynamic open systems' should be managed differently. For records in a **'static open system'**, public offices should take the following measures:

---

[5] Attempting to regenerate the database to apply retention and disposal practices at the individual record level in a 'closed system' would be very costly. A more effective option is to set a retention period at the database level.

- In consultation with the Arkib Negara Malaysia, prescribe a retention period for the records generated in the system based on operational, legal, fiscal and archival requirements and disposal arrangements.
- Ensure that indefinite retention of records is by exception only and, in cases where this is required, establish a review cycle to ensure the ongoing integrity of the records.
- Ensure that related system documentation and paper records are accounted for in the records retention and disposal schedule.
- Link the records to the appropriate area of the public offices' records classification system based on cross-references in the classification system and in the retention and disposal schedule completed for the records.
- Confirm that retention and disposal requirements have been incorporated into design of the system and, where necessary, enhance or redesign the system (public offices should follow the procedures in this Section to redesign the system).
- Check the integrity of the records according to the review cycles specified in the retention and disposal schedule.
- Review the records retention and disposal schedule periodically to ensure that the review cycle is appropriate and, if necessary, amend the schedule.
- Retain and dispose of the records, related system documentation and paper records in accordance with the retention and disposal schedule agreed by the Arkib Negara Malaysia.

The management strategy and procedures for **'dynamic open systems'** are generally the same as those for 'static open systems'. However, given the continuous removal and/or updating of records in a 'dynamic open system', the following should be adopted in addition to the measures given above:[6]

- Analyze the business processes and their related transactions to identify where records would be expected to be created and for how long they would be expected to be retained.
- Review the existing processes and transactions to see if records are being created and retained in accordance with the results of the analysis.
- Take the steps required to ensure that the system design is adjusted accordingly.
- Conduct reviews or audits on a regular basis in accordance with the system audit process to ensure that the retention and disposal specifications are followed through time.

If an **'open system'** is to be closed or defunct very soon, public offices should follow the procedures for 'closed systems' in managing the retention and disposal of the records in the system.

---

[6] Two examples of the retention period for records in 'dynamic open system' are given below for illustration: Example 1 – 'Completed electronic application forms to be kept for 10 years after rejection or approval of the license; copies of approved license notifications to be kept for 5 years; copies of rejected license applications to be kept for 2 years and then destroyed'. Example 2 – 'All paper and electronic records associated with the processing of an application for a license will be held for 5 years after the approval or rejection of the license and then destroyed'.

For destruction of classified electronic records stored in computer systems, public offices should ensure that the records are completely cleared from the storage media. If this is not feasible, the storage media must be physically destroyed to prevent the recovery of the classified information. For details, public offices should refer to the appropriate security standards and guidelines.

Preservation

Unlike paper-based records, electronic records can be subject to loss very easily because of the following factors:
- The fragility of the recording media (e.g. magnetic types and diskettes, optical discs, CD's, etc.).
- Dependency upon a technology environment that may render the records inaccessible because of changes to the technology.
- Insufficient metadata to explain the context of their creation, including why they were created, by who, why, when, where, etc.; this could render the content of the electronic records difficult to understand.

Public offices should contact the Arkib Negara Malaysia for information concerning the potential archival value of the records and, if required, establish an appropriate preservation strategy for the records. Records in an application system (regardless of the type of the system) required to be preserved for the long term should be managed in accordance with the procedures described below:
- Store electronic records on stable media and manage their integrity through time. For guidance on the management of storage media for electronic records, public offices should refer to Appendix 2.
- Store sufficient system documentation to ensure ongoing readability, accessibility, and understandability of the records during the length of time they are to be retained.
- For electronic records that are expected to be migrated to a new or substantially modified hardware/software platform and for which the records are required to be authentic and accessible in spite of the migration the following options are available:
  o **Transfer to paper or microfilm:** this is the oldest method of migration and has been used effectively for <u>textual documents</u> that may be retrieved and read, but that will not be altered and reused. However, paper and microfilm cannot capture the content of some types of information, such as animation, video and audio clips.
  o **Store records in a 'software-independent' format or a format that complies with open standards**: this strategy involves transferring electronic records to a 'software independent' format prior to storage, such as the use of eXtensible Mark-up Language (XML) or open text format.
  o **Retain records in their native software environment**: this strategy involves retaining electronic records for as long as possible in the hardware and software platform that was used to create them. This may be the only strategy available for preserving records in very specialized formats that cannot be accessed without the original software.

- o **Store records in more than one format**: this can reduce the uncertainty of software obsolescence and increase the options for future migration. This may be a sensible approach if no open standards exist and where several software products are competing for market share. Many systems today provide the capability to export records in two or more formats so that special conversion is not needed.
- For records that are to be converted from one form to another, ensure that the converted records continue to reflect requirements for authenticity. Factors to consider include the following:
    - o The structure and presentation of the records (i.e. it must be replicated to the extent required to enable the records to remain as evidence of the transactions that generated them).
    - o The adequacy of the descriptive information (i.e. metadata) required to enable the records to be linked to the context of their original creation;
    - o The systems environment into which the electronic records are being migrated (i.e. it must be of sufficient integrity and quality to enable the records to continue serving as evidence).
    - o Accountability for the integrity of the system and the records generated in the system (i.e. it must be migrated along with the records).

Appendix 1

Electronic Records Requirements[7]

In order to support the business and accountability requirements of Public offices, electronic records must be able to provide evidence of a decision or activity. Electronic records will only be evidence if the content, context, and structure information required to satisfy the requirements for record keeping are captured, maintained and made usable.

The requirements for record keeping that are described in the following section are general requirements that can be used for any given program or system. They represent a set of conditions that must be met if electronic records are to be authentic and reliable and to serve the purposes for which they were created and retained. They are in the form of a checklist that can be used by program managers and staff, applications systems developers, registry staff, LAN administrators, web masters and others to assess the extent to which these conditions are being met for the capture, maintenance, and preservation of electronic records.

1. Records are captured

Records have been created by all business transactions.

- Communications in the conduct of business between two people, between a person and a store of information available to others, and between a source of information and a person, generate a record.
- Data interchanged within and between computers under the control of software employed in the conduct of business created a record

Records are identifiable. They are related to a transaction which used all the data in the record and only that data.

- There exists a discrete record, representing the sum of all communications associated with a business transaction.
- All data in the record belongs to the same transaction.
- Each record is uniquely identified.

Records are complete. They contain the content, structure and context generated by the transaction they document.

---

[7] The following conditions were adapted from the "Pittsburgh requirements" developed as a result of the project, *Business Acceptable Communications* (also known as the Pittsburgh Project), University of Pittsburgh, 1989-1993.

Records are accurate. The content of records is quality controlled at input to ensure that information in the system correctly reflects what was communicated in the transaction.

Records are understandable. The relationship between elements of information content is represented in a way that supports their intended meaning.

Records are meaningful. The contextual linkages of records are in place to carry information necessary to correctly understand the transactions that created and used them.

- The business rules for transactions, which minimally locate the transaction within a business function, are maintained.
- A representation of the source and time of the transaction which generated a record is maintained.
- Links between records which comprised a business activity are retained.

Records are authentic. Authorized records creators originated all records.

- All records have creators which are documented.
- Records creators have been authorized to engage in the business transaction that generated the records.

2. Records are maintained

Records are preserved. The records continue to reflect content, structure and context within any systems by which the record are retained over time.

Records are inviolate. Records are protected from accidental or intended damage or destruction and from any modification.

- Data within a record are not deleted, altered or lost once the transaction which generated it has occurred.

Records are coherent. The information content and structure of records is retained in re-constructible relations.

- If records are migrated to new software environments, content, structure and context information are linked to software functionality that preserves their executable connections or representations of their relations thus enabling humans to reconstruct the relations that pertained in the original software environment.
- Logical record boundaries are preserved regardless of physical representations.

Records are auditable. The context of the records represents all processes in which the records participated.

- All uses of records are transactions.
- Transactions which index, classify, schedule, file, view, copy, distribute, or move a record without altering it are documented by audit trails attached to the original record.
- Transactions which execute a records disposition instruction whether for retention or destruction are documented by audit trails attached to the original record.

Records are removable. The record's content and the structure supporting the meaning of the content may be deleted by authorized individuals (i.e. in accordance with approved retention and disposal schedules).

- Authority for deletion of record content and structure exists.
- Deletion transactions are documented as audit trails.
- Deletion transactions remove the content and structural information of records without removing audit trails reflecting context.

3. Records are usable

Records are exportable. Records may be transmitted to other systems without loss of information.

- The export import facility has facilities to determine the elements of records metadata, the record content, the associated history data, etc and the sequence that is exported and then imported.
- Exporting protocols are reversible or the lost functionality is represented in a fashion that produces the same result in the target system as in the originating environment.

Records are accessible. It is possible to output record content, structure and context.

Records are available. It is possible to retrieve records.

Records are renderable. Records are displayed, printed or abstractly represented as they originally appeared at the time of creation and initial receipt.

- The structure of data in a record appears to subsequent users as it appeared to the recipient of the record in the original transaction or a human meaningful representation of that original rendering accompanies the presentation of the original content.

Records are evidential.

- Records reflect the context of their creation and use.
- Human meaningful representation of the contextual audit trail of a record accompanies all displays or printed output.

Records are redactable? Records are masked when it is necessary to deliver censored copies and the version as released is documented in a linked transaction.

- The release of redacted versions of a record is a discrete business transaction.
- The fact of the release of a redacted version of a record is an auditable use of the original record and therefore results in creation of an audit trail with a link to the transaction which released the redaction.

These conditions must be met if the records required in support of the business and accountability requirements of a public office are to be captured, used, and maintained as authentic and reliable records through time.

Appendix 2

Managing Storage Media for Electronic Records

I. Selection of suitable media

The storage media chosen should be stable and fully compatible with the information retrieval system. Floppy disks should not be used to store e-mail records of long-term or permanent value.

II. Media labeling

The removable storage media should be identifiable by external labels with sufficient information about the media and records stored therein. Such identification information may include:

- Unique identifier of each tape/disk/disc.
- Name of the organizational unit responsible for the record.
- Descriptive title of the content.
- Date of creation.
- Security grading.
- Type of copy, i.e. master or backup.
- Operating environment, i.e. hardware and operating software.
- Name and version number of the software which creates the attachment.
- Manufacture date of the storage medium.
- Storage location.

Label contents of the media should be written before attaching the labels to magnetic and optical media. Soft felt-tip markers should be used to prepare the label contents to avoid debris and scratches.

III. Handling and storage of the media

The storage media should be handled by their edges and kept away from dust, smoke, heat, direct sunlight and strong magnetic field. Magnetic and optical media should be shelved in an upright, vertical position to prevent warping of containers. They should be kept in protective containers when not in use.

Electronic records of long-term or permanent value are best preserved in an appropriate storage environment with 24-hour air conditioning and controlled temperature and humidity at 18°C ± 2°C and RH 40% ± 5% respectively. For assistance in storing long-term or permanent e-mail records, Departments should contact the National Archives.

Departments should provide proper access control and fire fighting equipment and facilities in the storage area to protect the physical security of the media.

At present, the physical life span of electronic media is still debatable and technology obsolescence also complicates the preservation of electronic records. Departments should thus develop strategies for system migration and implement a proper copying cycle to transfer their e-mail records, especially those requiring long-term or permanent retention, from old media to new media (e.g. from old CD-ROM to new CD-ROM). Normally the interval for media copying should be set for less than 10 years.

IV. Frequent checking of the media

Departments should check samples of the tapes/disks/discs at regular intervals to ensure the integrity of the media and see that the information is retrievable. Should any signs of deterioration be found, the records should be copied to tested tapes/disks/discs as soon as possible.

At present, the physical life span of electronic media is still debatable and technology obsolescence also complicates the preservation of electronic records. Departments should thus develop strategies for system migration and implement a proper copying cycle to transfer their e-mail records, especially those requiring long-term or permanent retention, from old media to new media (e.g. from old CD-ROM to new CD-ROM). Normally the interval for media copying should be set for less than 10 years.

V.   Types of magnetic media

The term 'magnetic media' is used to describe any record format where information is recorded and retrieved in the form of a magnetic signal.

The common types of magnetic media are:

- magnetic tape, including audio cassettes and reel-to-reel tapes, videotapes, computer tapes both on open reels and in cassettes, and tapes used in digital recording processes;

- magnetic hard disks; and

- magnetic floppy disks or diskettes.

VI.   Composition of magnetic media

Magnetic tape consists of a carrier of plastic film coated with a matrix containing magnetisable particles. The matrix also contains a plastic or resin binder, and other ingredients such as lubricants and fungicides. Sometimes the tape is coated on the reverse side with an antistatic material to reduce the build-up of static charges, and to improve its winding capability.

Magnetic hard disks have a metallic base, usually of aluminium. The base is coated on both sides with a matrix similar to that of magnetic tape.

Disk packs, which have a wide application in computing, consist of a number of hard disks stacked together around a central spindle. They require a special recording and playback system with many pairs of read/write heads.

Floppy disks and diskettes consist of a plastic base with a magnetic matrix on one or both sides. They are enclosed in a rigid, plastic protective jacket, which does not easily flex or bend. A slot in the jacket allows the read and write head to make contact with the disk.

VII.   Deterioration of magnetic media

All materials degrade over time. We cannot control this inevitable deterioration, but we can slow it down.

Some materials are inherently prone to deterioration, while others will only significantly degrade if they are stored in poor environmental conditions.

Below are examples of the types of deterioration to which magnetic media are prone:

▪ The tape carrier can become brittle and easily broken. The matrix on tapes and disks can deteriorate and subsequently flake off the base.

▪ The particles which retain the coded information in the magnetic layer can become unstable, leading to a gradual loss of signal quality and eventually to total information loss.

▪ Print-through, which is the transfer of a signal from one loop of tape onto an adjacent loop, occurs when tapes are stored for long periods without being played or exercised. The result is poor signal quality.

▪ Fluctuation and high levels of temperature and humidity may cause the magnetic and base layers to separate, or cause adjacent layers in a reel of tape to block together. High temperatures may also weaken the magnetic signal, and ultimately completely demagnetize the magnetic layer.

▪ Tapes are particularly susceptible to mould because pockets of air trapped in the windings can create microclimates which will support mould growth.

▪ Exposure of the magnetic layer to dust particles, dirt, grease and chemical pollutants can promote moisture condensation and oxidative deterioration. These contaminants also interfere with the contact between the playback head and the tape, resulting in a weakening of the recording or playback signal.

VIII. Magnetic fields

Because magnetic media store information by the alignment of magnetic particles, even a small external magnetic field can cause information loss on a tape or disk if it is in close proximity for long enough. Magnetic fields can be generated by items such as fridge magnets, magnetic screwdrivers and most machines with electric motors.

The degree of risk depends on several main factors: how close the media is to the source of the field; the strength of the field; and the duration of exposure. The effect of a magnetic field decreases with distance. This means that running a vacuum cleaner past the shelves will probably not cause any damage, whereas storing tapes or disks close to a large electrical generator could result in serious loss.

IX. Handling

Always handle magnetic media as carefully as possible.

Pick up magnetic tapes by their protective cases; do not touch the tape.

Wear lint-free gloves, or ensure that hands are clean and dry.

Support open-reel tapes by the hub during handling and transportation.

Disks should never be flexed, bent or picked up by the oval slot in their jackets, or by the centre hole of the disk.

Labeling should be in ink rather than pencil, as graphite dust from the pencil could interfere with the reading of the disk or tape. Once applied, labels should not be written on, and should only be attached to a protective case, rather than directly onto the magnetic tape or disk.

Only remove items from their protective packaging for immediate use, and always return them to their containers directly after use.

Cassettes and tapes should be wound to the end of one side after use. They should never be left in a partly wound state for any length of time, and the use of the 'pause' mode should be avoided.

Special care should be taken when moving magnetic media. Ensure that the media are not bumped or dropped, and that they are properly packed in custom-made transportation canisters. For the transport of large quantities or important material, consult freight and courier companies who specialise in magnetic media.

X.   Protective packaging

Paper and cardboard enclosures are unsuitable for the storage of magnetic media, as they tend to generate dust.

Tapes should be stored in cases made of non-magnetic material, preferably an inert plastic such as polypropylene. Polyvinylchloride (PVC) is unsuitable because it contains substances that may be damaging. Cases should have fittings to hold the tapes in position by the hub. They should be strong enough to protect the cassettes from physical damage, and they should close tightly to keep out dust particles.

Reels or cores used for winding tapes should be clean and free from cracks or sharp edges. There should be slots in the flanges of the reels to prevent bubbles of air from being trapped between the layers of tape on the reel. Reels should be made of aluminum or a stable plastic such as polypropylene (not PVC).

Floppy disks and diskettes should be stored in protective envelopes that have a non-abrasive surface and are resistant to the build-up of static electricity. Special envelopes are widely available and are suitable for this purpose.

XI. Storage requirements

Qualified staff should check storage areas to ensure the absence of magnets or magnetic fields that exceed acceptable limits. Walls, floors, wiring, and all storage and electrical equipment within the area must also be checked.

Storage areas should be free from potential sources of dust, such as typewriters, paper shredders, printers and carpet. Measures, such as the installation of an air lock, or the maintenance of positive internal air pressure, should also be taken to prevent dust entering from the outside.

Magnetic media should ideally be stored in closed metal cabinets to provide extra protection against heat and dust. However, if adequate environmental controls are in place, storage on open shelves and racks is acceptable. All storage equipment should be sturdy, allow tapes and disks to be stored vertically, and most importantly, be electrically grounded.

XII. Storage environment

Magnetic media should be stored in a temperature and relative humidity range of 18-20°C, and 35-40%, respectively. Under these conditions the natural deterioration of the objects can be slowed. In some instances deterioration can be further slowed by storage under lower temperatures. It is important that these environmental levels are stable. Mould will start to grow at around 60% relative humidity, and if the humidity fluctuates more than 10% in 24 hours or the temperature is too high, the items will be subjected to physical stresses that will accelerate their deterioration.

Exposure to ultraviolet (UV) light will also hasten degradation. Fluorescent tubes with UV-filters should be used wherever possible in storage areas, and turned off when not in use. UV light can be easily measured with a light meter, and levels should not exceed 75µW/lumen. An ideal storage area would have no windows, but if windows are present they should be covered with curtains or blinds.

Cleanliness is very important in records storage areas, both for the sake of the records, and from an occupational health and safety perspective. Never allow food or drink to be taken into a records storage area, and ensure the area is cleaned regularly. Insects and rodents, once attracted to a records storage area by food, may begin to eat the records.

Dust, heat and moisture can cause irreversible damage to magnetic media. Therefore storage areas should be fitted with special alarm systems, such as VESDA (Very Early Smoke Detection Alarm). Use of these systems can provide much earlier warnings of fire or high dust levels than conventional detection systems, and also minimise the need for large amounts of water to enter the storage area in the case of a fire. Fire detection and suppression technology is rapidly developing, and advice should be sought at the time the system is required to ensure the best method is employed.

XIII. Maintenance

The information held on magnetic media can only be processed or read by mechanical means, therefore it is essential that equipment is maintained in good condition: the use of poorly maintained equipment can actually cause damage to records.. The heads, disk drive and tape drive elements of playback and recording equipment should be cleaned regularly according to manufacturers' recommendations.

Some tape manufacturers also recommend the exercising of tapes to improve their life span. Problems, such as creases or folds in the tape, may build up as the tape pack sits in storage. Exercising can reduce the stresses that cause these problems and may also reduce the danger of print-through.

Exercising involves winding the tape slowly through its entire length at playback speed, without stopping. The process should be carried out in the same environmental conditions in which the tapes are to be stored. Tapes which are to be moved to a different environment for exercising should be allowed a period of 24 hours to acclimatize to the new environment before exercising them. It is generally recommended that exercising be carried out at least every three years.

XIV. Reformatting and data migration

To minimize deterioration due to handling and use, copies of important and frequently used tapes should be made for reference purposes. Ideally, a preservation master copy, a duplicating copy and a reference copy should be produced, and clearly labeled as such., As a disaster preparedness measure, the preservation master copy should be stored in a different location to the others. The duplicating copy may be used to produce further reference copies when required.

Long-term preservation of magnetic media is affected by two major factors: the intrinsic instability of the media; and the likelihood of the hardware required to read the media becoming unavailable. Even if tapes or disks made today are in excellent condition in 30 years time, the machines required to play them will almost certainly have been superseded long before, and for all practical purposes the records will be unusable. Beta format videotapes are a good example of this problem. Once very common, they have now been entirely superseded by VHS format tapes and it will soon be very difficult to view a Beta video.

The main prospect for long-term retention of the information held on magnetic media seems to be in regular copying or data migration, thus maintaining a good quality signal that can be read using available equipment. Copying can either be to fresh tape or disk, or to some other machine-readable format such as CD-ROM.

Copying to analog tape will involve some loss of signal quality at every copying stage. This may be significant after as few as two or three copies. The problem may be overcome by copying to a digital format such as digital tape (DAT for audio tapes) or optical disk. The tape used for digital recording is no more permanent than the tape used for analog recordings but the information can be copied many times without a significant loss of quality. The problem does not arise with computer tapes as they are already recorded digitally.

Digital recording hardware is expensive. To minimize costs you can record initially on analog tape and then transfer to a digital medium for archiving. You should consider whether the information will need to remain on magnetic media permanently, or whether a paper or microfilm format would be a better way of retaining the information. Paper-based records and microfilm will always last longer than magnetic records stored in the same conditions.