the national archives

Generic requirements for sustaining electronic information over time:

2. Sustaining authentic and reliable records: management requirements

TABLE OF CONTENTS

1 Introduction

1.1.1 Sustainable records are defined as those electronic objects and their concomitant metadata which defines them as records, which require continued retention by the creating or owning organisation until such time as the records can be destroyed or, where that is warranted, passed to a specialist archive for permanent archiving. If records are to be sustained there must be confidence that the maintained records possess authenticity, reliability, integrity and usability.

1.1.2 This *document* should be read in conjunction with the other three accompanying volumes in the series on *Generic requirements for sustaining electronic information over time*. The titles of the other 3 volumes in the series are:

1. *Defining the characteristics for authentic records*
3. *Sustaining authentic and reliable records: technical requirements*
4. *Guidance for categorising records to identify sustainable requirements*

1.1.3 Volume 1 provides a summation of the principles and attributes, which would support an attestation of authenticity and integrity and which need to be maintained as part of the electronic record in accordance with *BS ISO 15489 Information and documentation – Records management standard*. Volume 3 addresses the technical requirements needed to maintain sustainable electronic records. Volume 4 provides high-level guidance for departments seeking to categorise their records to scope the specific nature of the requirements needed to sustain these record categories as authentic records.

1.1.4 This document defines the key elements that should be incorporated within any management strategic planning framework and the processes that will also have to be developed and supported in order to ensure that electronic records which are to be sustained over a defined period of time are able to satisfy the characteristics of a record as defined in *BS ISO 15489* that is authenticity, reliability, integrity and usability. If these characteristics are not maintained the sustained records will lose credibility and will lose evidential value. This section of the generic requirements will define performance indicators and non-functional requirements as opposed to the technical management requirements which are described in Volume 3 of the *Generic requirements for sustaining electronic information over time - Sustaining authentic and reliable records: technical requirements.*

1.1.5 These generic requirements are not a full specification. They form a baseline, which sets out, - the minimum necessary to maintain credible electronic records which will continue to possess the attributes of authenticity and integrity over time. They also should be read as an accompaniment to the Functional Requirements for Electronic Records Management Systems 2002 revision: final version which are available at:

http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/default.htm

1.1.6 It is also recommended that any management process developed in response to the guidance given in this document should also be bench-marked against *BS ISI 7799* on information security.

1.1.7 The guidance is intended primarily for those working in central government; the principles will also be relevant in local government and throughout the public sector. Throughout this document the term ‘department’ should be taken to apply to any public sector organisation, including all departments, agencies and other organisations across government. Familiarity with the concepts of records as used in central government is assumed.

1.1.8 Each government organisation wishing to make use of these requirements, as a baseline or benchmark, will always need to consider its own specific business needs and context in determining its own requirements. These generic requirements must be tailored by: adding specialist business needs which are not covered at this generic level, selecting from alternative requirements according to corporate policy and practice, assessing whether any requirements listed in these volumes are highly desirable as opposed to mandatory for their own context

1.1.9 The generic functions described in this document may also be relevant to a permanent archive but the needs of archival preservation are considered as distinct from those operations required to maintain electronic records for continuing business needs even where the overall retention period may last for some decades.

2 Operational frameworks

2.1.1 In order to develop and implement appropriate strategies to sustain their electronic records organisations will first need to establish a framework, which will define the business needs which are supported by each group of records in their custody, the style and content of the metadata, which will accompany those records and an appropriate technical solution for each software format included in the collection. It will also be necessary to ensure reproduction of copies of records upon demand together with any functionality that the business purpose may require when accessing these records. It will also be necessary to determine the performance criteria for evaluating the success of any action implemented within the framework. Criteria for assessing such frameworks will include:

- definition of what an implementation plan will need to address
- establishment of the business need serviced by the records
- whether the business need has been met by the adopted strategy

2.1.2 The key element is defining the management processes that need to be identified and established within any organisation that proposes to maintain reliable records over a specific period. In order to do this departments will need to develop a document will describe the strategic framework and the accompanying criteria to determine the required activities needed to conserve and maintain the records. Such documents need to address the following points:

- what must be done,
- determine how it should be done
- define what the results should be

2.1.3 The tools provided here will define how successful sustainability strategies will be evolved, the mechanisms to ensure their continued relevance together with performance criteria to provide measures to assess the effectiveness of the process.

2.1.4 The management strategy will have to establish actions that must be executed either at specified times or under specified conditions. It will clarify and define the business purpose, and the technical requirements for maintaining the records in a form that enables that purpose. The document will have to provide performance criteria and quality indicators for the following sections.

2.2 Management Controls

2.2.1 Sustainability will be managed by producing a comprehensive framework consisting of sets of strategies and action plans. Each of these will be linked to a specific body of electronic records, categorised according to business requirements, which establish a need to maintain the records for a defined period. Each body of records will have a defined level of functionality with an identified technological infrastructure and methodology needed to implement the action plans.

2.2.2 The elements listed below should be used to scope the scale of the programme of work required to execute the sustainable strategy. The management process will also produce information about the maintenance function and about how the records are being sustained or preserved and this information should be used to refine and re-focus the strategy. It is also necessary to define the performance environment within which any preservation strategy will operate. The key elements to be addressed are:

- Identifying the records that require to be sustained
- External controls (e.g. applicable legalisation and regulations, management requirements)
- Defining the nature of the products (e.g. the standard and form of the records that are to be sustained
- Resources required to execute the strategy (e.g. personnel, infrastructure etc.)

2.2.3 These four components need to fully identified in every strategic framework with appropriate descriptions for each sub-element listed below.

Inputs

- Information about the content of electronic records required to be sustained
- Information about the nature and capability of the software to be sustained
- Management information and experience of sustainability (e.g. migration, configuration, emulation)

External environment and controls

- Institutional requirements (including any regulatory or statutory constraints)
- User access requirements
- Current IT/IS infrastructure

Products

- Criteria for assessing if the sustained records meet the business need
- Information about actively maintained records
- Priorities for sustainability and action plans
- Maintenance strategies
- Assessment of continued authenticity of records
- Proposed changes to technological infrastructure

Resources

- Dedicated facilities and infrastructure needed to deliver sustained records
- Personnel needed to sustain the records

2.2.4 The processes and mechanisms, which will need to be established to ensure the strategic framework is credible, are described in sections 2 through to 12 of this document.

2.2.5 It is strongly recommended that when developing these strategic frameworks that the accompanying volumes of these generic requirements are also referenced; *Volume 3 Sustaining authentic and reliable records: technical requirements* and *Volume 4 Guidance for categorising records to identify sustainable requirements* to ensure the strategy takes account of all the issues involved in maintaining electronic records in accordance with *BS ISO 15489 Information and documentation – Records management standard* to ensure the characteristics of a record as defined in *BS ISO 15489* that is authenticity, reliability, integrity and usability are appropriately supported. If these characteristics are not maintained the sustained records will lose credibility and will lose evidential value and the value of the asset to the department will diminish substantially.

3 Determining the appropriate maintenance environment

3.1.1 Identifying the relevant regime to maintain records in an appropriate environment entails identifying the classes or categories of objects that must be maintained. This includes specifying, for each category, the attributes and methods that must be preserved, as well as any requirements for certifying that any reproduced record is authentic.

3.1.2 Evolution of a requirement will be guided by evaluation of prior experience in applying such requirements to records that have been transferred to a sustained environment. The result of this process will be an informed and enhanced requirement, where the specification consists in identifying what operational, institutional and regulatory requirements apply to what records and how each applicable requirement is to be implemented.

3.1.3 A coherent set of requirements for maintaining electronic records in a manner which will enable reproduction of the records and where this is required certification of the authenticity of the reproduced records. Each set of requirements will apply to a specified collection of digital objects or records. The requirements encompass both the:

- the digital objects themselves
- record collections, categories or classes
- storage media to be used the maintenance of digital files

3.2 Performance measures for maintained records

3.2.1 Requirements for media include:

- standards and specifications of what media are to be used and for what purpose
- how volumes are to be labelled
- and how physical files are to be written

3.2.2 Requirements for digital objects include:

- how both physical and logical files are to be identified
- how logical files are mapped to physical files
- how integrity of a file is ensured
- specifications for appropriate software file formats
- criteria for assessing and selecting current and future media and software file formats

3.2.3 Requirements for record collections include:

- how records are to be composed from digital components
- how records in an archival aggregate are to be arranged

- how the business needs and concomitant maintenance need of records are to be expressed, captured and stored

4 Maintaining effective records – the role of a technology watch programme

4.1.1 Effective storage of electronic records requires a pro-active regime to maintain the records are always available and held on appropriate formats, to ensure the records persist over time in a reliable and an authentic form. In order to achieve effective storage the custodial organisation needs to establish a technology watch or monitoring programme. Such a programme will need to continuously monitor the current software and hardware environment prevailing to ascertain if any of the software file formats, within which the records are held, and the storage media within which the records are stored are in some way obsolescent or problematic. For example it may no longer be possible to support a particular software format without disproportionate cost and migration to another software format may be seen as the viable solution. Similarly the storage media may need to be change as it is obsolescent and the records will require to be written to the new preferred storage format.

4.1.2 The programme will need to establish procedures for determining when such an issue has arisen and processes to determine what action should be taken. Depending on the nature of the problem it may be necessary to migrate certain record collections to a later version of the same software format or even to another format altogether. Similarly the storage media will need to be replaced with a different media type periodically as technology changes and a migration project to move to the new storage media should be undertaken before accessing the older storage media becomes problematic.

4.1.3 The elements of a technology watch programme, which will define effective maintenance, are;

- identifying the mechanisms to effectively monitor the viability of the formats upon which the record components are held
- identifying the criteria for assessing whether a particular format requires intervention
- determining what type of intervention is required
    - maintaining existing technology
    - developing and maintaining appropriate emulators
    - migrating to current version of existing formats
    - conversion to standard industry supported formats
    - transformation to a persistent format
    - rendering to a new format to provide increased functionality
- identifying an appropriate time-scale to ensure the required resource is available to undertake the necessary work before the records are irretrievably compromised
- identifying criteria to evaluate whether the intervention has been successful
- determine minimum information levels to be captured within the management audit trail for each process

- establish criteria for assessing if a particular process has been successful

4.2 Capture into a secure record-keeping environment

4.2.1 Capturing the record within the electronic environment involves management of the interface between the record-keeping system and the applications, such as word processors or e-mail clients, which are used to create or receive records. Systematic capture requires both a technical interface and a set of rules or procedures, which govern its behaviour and successful application within the organisation. Maintenance of sustainable records requires that records should have been captured upon creation into a managed environment and these controls should continue to apply for as long as the record is required by the organisation.

4.2.2 However there will be cases where it is necessary to maintain records created in an unmanaged environment (that is held outside of an EDRMS environment). In such a case they should be imported into a managed environment where the mechanisms of sustainability can be applied and recorded. The record of capture will need to be annotated to record the circumstances in which the records were created and stored until their formal capture into a managed environment.

4.2.3 Depending on the business need for capture from such environments it may be useful to look at the example provided by forensic IT investigation, which is predicated on the capture of data from systems in a legally-admissible form. Within the United Kingdom the recommended basis for such procedures are the various codes of practice published by the British Standards Institution (BSi) - ref. *DISC PD 0008:1999* and *DISC PD 5000 - 1-6:2002*.

4.2.4 The mechanisms for capture should ensure that:

- appropriate records are captured. There should be a clear understanding of the information which should be captured as a record, and the operational means of identifying and capturing this within the working environment
- all types of record are captured. Workable mechanisms should exist for all record-creating applications in use to enable the capture of records from that application according to approved formats and standards
- complete records are captured. Capture mechanisms should be capable of acquiring all the elements which make up a record, and associating these together in a meaningful and useful manner
- metadata is captured and associated with records from the time of their creation, and that this descriptive metadata is closely bound with the record itself
- links to other records are established and maintained, within broader record assemblies, including mixed electronic and paper assemblies, and in other classification mechanisms if appropriate.

4.2.5 The above requirements emerged in the definition of the *Requirements for Electronic Records Management Systems: Functional Requirements* – Revision 2002 published by the National Archives (TNA) Those requirements

are relevant where a sustainable records policy is to be applied. Other typical requirements for electronic records management, which will also apply in a managed maintenance environment, are:

- capturing, storing, indexing and retrieving all elements of the record as a complex unit, and for all types of record
- management of records within class categories or filing structures to maintain the narrative links between records
- record level metadata describing contextual information
- integration between electronic and paper records
- secure storage and management to ensure authenticity and accountability, including support for legal and regulatory requirements
- appraisal and selection of records for preservation and transfer to the keeping of the National Archives (TNA) or other permanent archive
- systematic retention and disposition of records
- migration and export of records for permanent preservation.

4.2.6 All records upon capture into a managed environment should meet the minimum registration requirement specified in *BS ISO 15489* which specifies the following metadata as a minimum:

- a unique identifier assigned from the system
- the data and time of registration
- a title or abbreviated description
- the author (person or corporate body), sender or recipient

4.2.7 The *Requirements for Electronic Records Management Systems Functional Requirements 2002 revision: final version* provides much of the requisite functionality that is needed if records are to be pro-actively sustained and the *Requirements for Electronic Records Management Systems Metadata Standard describes the required metadata elements.*

5 Record attributes and linkages to records

5.1.1 The presumption of a record's authenticity is strengthened by knowledge of certain basic facts about it. The attributes identified in these requirements embody those facts. The requirement that the attributes be expressed explicitly and linked inextricably to the record during its life, and carried forward with it over time and space, reflects a need that such expression and linkage provide a strong foundation on which to establish a record's identity and demonstrate its integrity.

5.1.2 The link between the record and the attributes is a conceptual rather than a physical one, and the requirement could be satisfied in different ways, depending on the nature of the electronic system in which the record resides. In an ERMS, this requirement is usually met through the creation of a record profile. When a record is exported from the live system, migrated in a system update, or transferred to an external specialist archive, the attributes should be linked to the record and available to the user. When pulling together the data prior to export, the creator should also ensure that the data captured is the right data.

5.1.3 To support a presumption of authenticity the custodian must possess, obtain and maintain evidence that the following metadata attributes defined in the *Requirements for Electronic Records Management Systems Metadata Standard* are supported:

- Identifier System ID
- Title
- Creator
- Date Created
- Date Acquired (mandatory for e-mail)
- Date Declared
- Addressee (mandatory for e-mail)
- Type Record type (mandatory where applicable)
- Relation Copy (pointer) (mandatory where applicable)
- Relation Parent object
- Relation Redaction/Extract (mandatory where applicable)
- Relation Reason for redaction/extract (mandatory where applicable)
- Relation Rendition (mandatory where applicable)
- Aggregation
- Rights Protective marking

5.1.4 To support a presumption of integrity the custodian must possess or obtain evidence that the following attributes are supported:

- name of the creating organisation that regards the record as part of its official corporate record
- name of the organisation which has custody of the record (if different from the creating organisation)
- indication of types of annotations added to the record
- indication of technical modifications

6 Access Management

6.1.1 Defining access privileges means assigning responsibility for the creation, modification, annotation, relocation, and destruction of records on the basis of competence, which is the authority and capacity to carry out an administrative action. Implementing access privileges means conferring exclusive capability to exercise such responsibility. In electronic systems, access privileges are usually articulated in tables of user profiles. Effective implementation of access privileges involves the monitoring of access through an audit trail that records every interaction that an officer has with each record (with the possible exception of viewing the record).

6.1.2 The creator has to define and effectively implement access privileges concerning the creation, modification, annotation, relocation, and destruction of records.

6.1.3 The custodian has to maintain and update and where necessary extend existing access privileges to implement all changes relating to modification, annotation, relocation, and destruction of records.

7 Technical modifications

7.1.1 Technical modifications are any changes in the digital components of the record. Such modifications would include any changes in the way any elements of the record are digitally encoded and changes in the methods applied (e.g. software) to reproduce the record from the stored digital components; that is, any changes that might raise questions as to whether the reproduced record is the same as it would have been before the technical modification. The indication of modifications might refer to additional documentation external to the record that explains in more detail the nature of those modifications.

7.1.2 The reason for any modification has to be fully documented as must the nature and date of application of a specific process together with references of the records, objects or components that have been subject to modification. It is essential that this information be incorporated within the database charged with the management oversight of the records being sustained or preserved by the custodian.

7.2 Protective Procedures: documenting management of loss and corruption

7.2.1 Procedures to protect records against loss or corruption include: prescribing regular back-up copies of records and their attributes; maintaining a system back-up that includes system programs, operating system files, etc.; maintaining an audit trail of additions and changes to records since the last periodic back-up; following any system failure ensuring that the back-up and recovery procedures will automatically guarantee that all complete updates (records and any control information such as indexes required to access the records) contained in the audit trail are reflected in the rebuilt files and also guarantee that any incomplete operation is backed up. The capability should be provided to rebuild forward from any back-up copy, using the back-up copy and all subsequent audit trails.

7.2.2 The creator or custodian has to establish and effectively implement procedures to prevent, discover, and correct loss or corruption of records;

7.3 Protective Procedures: Media and Technology

7.3.1 Procedures to counteract media fragility and technological obsolescence include: planning upgrades to the organisation’s technology base; ensuring the ability to retrieve, access, and use stored records when components of the electronic system are changed; refreshing the records by regularly moving them from one storage medium to another; and migrating records from an obsolescent technology to a new technology.

7.3.2 The creator or custodian has to establish and effectively implement procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change.

7.4 Media Refreshment and Migration

7.4.1 To avoid loss or corruption of the records through degradation of the storage media over time it will be necessary to establish a media refreshment regime which will involve re-writing the records to the same media type required by the storage strategy to ensure continued readability. This needs to be undertaken at regular intervals in accordance with the timescales determined in the storage strategy. These intervals should not however exceed the periods recommended by the manufacturers of the media for the refreshment of that type of media.

7.4.2 When it is determined that the storage media currently used by the custodian to hold the records is no longer an appropriate storage medium (e.g. the existing media is considered to potentially obsolescent) a media migration exercise should be undertaken. Media migration differs from media refreshment in that the records are re-written to a different storage media from the one they were previously stored on. The new media type will have been identified as an appropriate replacement by the technology watch strategy. Following a successful media migration a new media refreshment scheme must be established and maintained as described above.

7.4.3 After selection and prior to refreshment or migration taking place, a new media handling process guide must be approved if an appropriate one does not already exist.

7.4.4 The process must dispose of any failing or ageing media in a managed and secure fashion so that:

- the media will not normally come into the possession of any unauthorised third party
- in the event that they should come into the possession of any unauthorised third party, the media should be overwritten so that no information can be retrieved
- a record of the event and of the method used to overwrite the media to be disposed should continue to be held on the system

7.4.5 Where the information is considered to be particularly sensitive or it is subject to a national security classification over writing of the media is not considered an adequate solution. The media should be physically destroyed as part of a controlled process. The Ministry of Defence has established procedures for the destruction of such media and departments are advised to seek the advice of their departmental security officers before any decision is taken. It should be noted that storage of highly classified electronic records should only arise where provision has been made for an appropriately secure network and care must be taken that records with high security classifications are not transferred onto systems which are inappropriate for that level of security.

8 Establishment of Document Types

8.1.1 The document type of a record as defined in the *Requirements for Electronic Records Management Systems Metadata Standard* may be determined in connection to a specific administrative procedure, or in connection to a specific phase(s) within a procedure. The document type or form may be prescribed by a business process or workflow, where each step in an administrative procedure is identified by a specific record or document type. If a creator customizes a specific application, such as an electronic mail application or template within MS Word for a pro-forma, to carry certain fields, the customized form becomes, by default, the required document type. It is assumed that the creating organisation, acting on the basis of its own needs or because of pre-existing statutory requirements, will establish the required document types for their records.

8.1.2 When the creator establishes the document type in connection to a procedure, or to specific phases of a procedure, that will allow for the maintenance of the authenticity of the record. As that determination will vary from one form of a record to another, and from one creating organisation to another, it is not possible to predetermine or generalise the relevance of specific elements of documentary form in relation to authenticity.

8.1.3 The creator or custodian has to establish the document types or forms of records associated with each procedure (e.g. templates, forms etc) either according to any legislative or regulatory requirements system or those of the creating organisation and ensure these are documented.

9 Authentication of Records

9.1.1 In common usage, to authenticate means, or serves, to prove the authenticity of something. More specifically, the term implies establishing genuineness by adducing legal or official documents or expert opinion. For the purposes of these requirements, authentication is understood to be a declaration of a record's authenticity at a specific point in time by a person entrusted with the authority to make such declaration. It may take the form of an authoritative statement (which may be in the form of words or symbols) where there is a specific legal provision for such a statement or it may take the form of a digital signature whose authenticity can be verified using the public key infrastructure (PKI). The effect of either method when added to or inserted into a copy of the record is to attest that the record is authentic. The requirement may also be met by linking the authentication of specific types of records to business procedures and assigning responsibility to a specific office or officer for authentication or by the adoption of enabling technology such as watermarking, digital or biometric signatures.

9.1.2 It should be emphasised that the adoption of such authentication methods described above should not normally be added to or inserted into the preserved record whereas it may be appropriate, or required, for the custodian to use one of these methods when providing an authenticated copy to a third party. If an authentication method is inserted into the preserved record this will change its attributes and could compromise the integrity of the record thereby calling into question its authenticity. Intrusive techniques such as watermarking may themselves compromise the authenticity of digital data, and certainly may not be sustainable over time. In general any technique, which alters the bit stream of the actual record held and maintained by the custodian should, be avoided.

9.1.3 The authentication of copies differs from the validation of the process of reproduction of the digital components of the records. The latter process occurs every time the records of the creator are moved from one medium to another or migrated from one technology to another.

9.1.4 Where authentication is required by statute or the needs of the organisation, the creator or custodian has to establish specific rules regarding which records must be authenticated, by whom, and the means of authentication.

9.2 Identification of Authoritative Record

9.2.1 An authoritative record is a record that is considered by the creator to be its official record and is usually subject to procedural controls that are not required for other copies. Normally any record subject to management by an ERMS has the capability of being an authoritative record but the organisation may regard certain document types (e.g. affidavits) as being especially authoritative as they are required to use them in discharge of statutory obligations. In such cases such a designation should be apparent in the record retention schedule applied to those records and the metadata designating an authoritative record should form part of the Rights and Mandate elements as defined in the Record Management Metadata Standard.

9.2.2 If multiple copies of the same record exist, the creator or custodian has to establish procedures that identify which record is considered authoritative.

9.2.3 It is understood that in certain circumstances there may be multiple authoritative copies of records, depending on the purpose for which the record is created.

10 Removal and Transfer of Relevant Documentation

10.1.1 Where there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from one platform to another system or an archive external to the organisation, the creating organisation has to establish and effectively implement procedures determining what documentation has to be removed and transferred to the new system which is to be maintained and preserved along with the records.

10.1.2 This requirement implies that the trusted custodian needs to carry forward with the removed records all the information that is necessary to establish the identity and demonstrate the integrity of those records, as well as the information necessary to place the records in their relevant contexts.

11 Controls over records, export, maintenance, and reproduction

11.1.1 The controls over the transfer (export) of electronic records across platforms include establishing, implementing, and monitoring procedures for registering the records' export; verifying the authority for export; examining the records to determine whether they correspond to the records that are designated in the terms and conditions governing their export; and formally importing the records onto the new platform.

11.1.2 As part of the export process, the assessment of the authenticity of the creator's records should be verified. This includes verifying that the attributes relating to the records' identity and integrity have been carried forward with them along with any relevant documentation.

11.1.3 The trusted custodian should establish access privileges concerning the access, use, and reproduction of records; establish procedures to prevent, discover, and correct loss or corruption of records, as well as procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change. Once established, the privileges and procedures should be effectively implemented and regularly monitored. If authentication of the records is required, the custodian should establish specific rules regarding who is authorized to authenticate them and the means of authentication that will be used.

11.1.4 The controls over the reproduction of records include establishing, implementing, and monitoring reproduction procedures that are capable of ensuring that the content of the record is not changed in the course of reproduction.

11.1.5 The procedures and system(s) used to transfer or export the records to another platform; maintain them in-situ; and reproduce them must provide adequate and effective controls to guarantee the records' identity and integrity, and specifically that:

- unbroken custody of the records is maintained;
- security and control procedures are implemented and monitored;
- the content of the record and any required annotations and elements of documentary form remain unchanged after reproduction.

12 Documentation of reproduction processes and outputs

12.1.1 Records in order to be access will require to be produced the existing software format or rendered or re-produced in another format such as XML or PDF. Documenting the reproduction process and its effects is an essential means of demonstrating that the reproduction process is transparent (i.e., free from pretence or deceit). Such transparency is necessary to the effective fulfillment of the preserver's role as a trusted custodian of the records. Documenting the reproduction process and its effects is also important for the users of records since the history of reproduction is an essential part of the history of the record itself. Documentation of the process and its effects provides users of the records with a critical tool for assessing and interpreting the records.

12.1.2 In those cases where a copy of a record is known not to fully and faithfully reproduce the elements expressing its identity and integrity, such information has to have been documented by the custodian and this documentation has to be readily accessible to the authorised user.

12.1.3 Reproduction includes viewing both rendition in the original software format and viewing of renditions in alternate formats determined as needful by the custodial organisation The activity of reproduction has to document:

- the date of the records' reproduction and the name of the responsible person
- the relationship between the records acquired from the creator and the copies produced by the custodian
- the impact of the reproduction process on their form, content, accessibility and use