InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems

International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records

APPENDIX 19

A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records

by

Luciana Duranti, The University of British Columbia
Jim Suderman, City of Toronto Archives
Malcolm Todd, National Archives of the United Kingdom

Status: Final (public)

Version: Electronic

Publication Date: 2008

Project Unit: Policy Cross-domain Task Force

URL: http://www.interpares.org/display_file.cfm?doc=ip2_book_appendix_19.pdf

How to Cite: Luciana Duranti, Jim Suderman and Malcolm Todd, "Appendix 19: A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008). <http://www.interpares.org/display_file.cfm?doc=ip2_book_appendix_19.pdf>

A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records[1]

Introduction

The InterPARES research projects have examined the creation, maintenance and preservation of digital records. A major finding of the research is that, to preserve trustworthy digital records (i.e., records that can be demonstrated to be reliable, accurate and authentic), records creators must create them in such a way that it is possible to maintain and preserve them. This entails that a relationship between a records creator[2] and its designated preserver[3] must begin at the time the records are created.[4]

The InterPARES 1 research (1999-2001) was undertaken from the viewpoint of the preserver. Three central findings emerged from it: 1) there are several requirements that should be in place in any recordkeeping environment aiming to create reliable and accurate digital records and to maintain authentic records;[5] 2) it is not possible to preserve digital records but only the ability to reproduce them;[6] and 3) the preserver needs to be involved with the records from the beginning of their lifecycle to be able to assert that the copies that will be selected for permanent preservation are indeed authentic copies of the creator's records.

The InterPARES 2 research (2002-2006) took the records creator's perspective. The researchers carried out case studies of records creation and maintenance in the artistic, scientific and governmental sectors; they modeled the many functions that make up records creation and maintenance and records preservation according to both the lifecycle and the continuum models; they reviewed and compared legislation and government policies from a number of different countries and at different levels of government, from the national to the municipal; they analyzed many metadata initiatives and developed a tool to identify the strengths and weaknesses of existing metadata schemas in relation to questions of reliability, accuracy and authenticity; and, once again, they studied the concept of trustworthiness and its components, reliability, accuracy

[1] The term initially used in the InterPARES Project is "electronic records." In fact, the book resulting from InterPARES 1 is named *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project* (Luciana Duranti, ed.; San Miniato, Archilab, 2005), and the formal title of InterPARES 2 carries that terminology forward. However, in the course of the research, the term "electronic record" began to be gradually replaced by the term "digital record," which has a less generic meaning, and by the end of the research cycle, the research team had developed separate definitions for the two terms and decided to use the latter as the one that better describes the object of InterPARES research. The definition for "electronic record" reads: "An analogue or digital record that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person." The definition for "digital record" is, effectively, a digitally-encoded object and the metadata necessary to order, structure or manifest the object's content and form, where "digital object" is taken to mean "a discrete aggregation of one or more bitstreams and the metadata about the properties of the object and, if applicable, methods of performing operations on the object." See the InterPARES 2 Terminology Database, available at http://www.interpares.org/ip2/ip2_terminology_db.cfm.

[2] Records creator is the physical or juridical person (i.e., a collection or succession of physical persons, such as an organization, a committee, or a position) who makes or receives and sets aside the records for action or reference. As such, the term includes all officers who work for a juridical person, such as records managers, records keepers and preservers.

[3] Records preserver is a generic term that refers more to the function than to the professional designation of the physical or juridical person in question. Thus, the preserver might be a unit in an organization, a stand-alone institution, an archivist or anyone else who has as primary responsibility the long-term preservation of records.

[4] Records are created when they are made or received and set aside or saved for action or reference.

[5] See Authenticity Task Force (2002). "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records," in *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Italy: Archilab, 2005), 204–219. Online reprint available at http://www.interpares.org/book/interpares_book_k_app02.pdf.

[6] See Kenneth Thibodeau et al., "Part Three – Trusting to Time: Preserving Authentic Records in the Long Term: Preservation Task Force Report," ibid, 99–116. Online reprint available at http://www.interpares.org/book/interpares_book_f_part3.pdf.

and authenticity and how it is understood, not just in the traditional legal and administrative environments, but in the arts, in the sciences and in the developing areas of e-government.

The case studies showed that record creation in the digital environment is almost never guided by considerations of preservation over the long term. As a result, the reliability, accuracy and authenticity of digital records can either not be established in the first place or not be demonstrated over periods of time relevant to the "business"[7] requirements for the records. These records cannot therefore support the creator's accountability requirements, nor can they be effectively relied upon either by the creator for reference or later action or by external users as sources. Furthermore, they cannot be understood within an historical context, thereby undermining the traditional role of preserving organizations such as public archival institutions.

The research undertaken in records and information-related legislation showed that no level of government in any country to date has taken a comprehensive view of the records lifecycle, and that, in some cases, legislation has established significant barriers to the effective preservation of digital records over the long term, most notably that regarding copyright.

It was the responsibility of the InterPARES 2 Policy Cross-domain research team (hereinafter "the Policy team") to determine whether it was possible to establish a framework of principles that could guide the creation of policies, strategies and standards, and that would be flexible enough to be useful in differing national environments, and consistent enough to be adopted in its entirety as a solid basis for any such document. In particular, such a framework had to balance different cultural, social and juridical perspectives on the issues of access to information, data privacy and intellectual property.

The findings of the InterPARES 1 research were confirmed by the research conducted by the InterPARES 2 Policy team, which further concluded that it is possible to develop such a framework of principles to support record creation, maintenance and preservation, regardless of jurisdiction. This document, in combination with other products of the Project, especially the Chain of Preservation (COP) model,[8] reflects this conclusion, while emphasizing the need to make explicit the nature of the relationship between records creators and preservers.

The Policy team developed two complementary sets of principles, one for records creators and one for records preservers, which are intended to support the establishment of the relationship between creators and preservers by demonstrating the nature of that relationship.[9] The principles for records creators are directed to the persons responsible for developing policies and strategies for the creation, maintenance and use of digital records within any kind of organization, and to national and international standards bodies. The principles for records preservers are directed to the persons responsible for developing policies and strategies for the long-term preservation of digital records within administrative units or institutions that have as their core mandate the preservation of the bodies of records created by persons, administrative units or organizations external to them, selected for permanent preservation under their jurisdiction for reasons of legal, administrative or historical accountability. They are therefore intended for administrative units (e.g., a bank, a city or a university archives) or institutions (e.g., a community archives or a state archives) with effective knowledge of records and records preservation.

[7] The term "business" is used in its most general sense, since the object of the InterPARES research includes works of art and scientific data as well as standard types of business records.

[8] The COP model is available in Appendix 14 and at http://www.interpares.org/ip2/ip2_models.cfm. A narrative discussion of the model is provided in the Modeling Cross-domain Task Force Report.

[9] The initial draft of the principles relied heavily on the contributions of three research assistants: Fiorella Foscarini, Emily O'Neill and Sherry Xie.

Structure of the Principles

The principles are similarly presented, with the principle statement followed by an explanatory narrative, sometimes with illustrative examples. The principles are more often phrased as recommendations ("should") rather than imperatives ("must"), because some of them might not be relevant to some records creators or preservers. Each principle statement is followed by an indication of the corresponding principle in the other set (C stands for Creator, P stands for Preserver; the number is the principle number in the C or the P set). The reason why the principle numbers do not correspond in the two sets (C1=P1) is that the principles are listed in each set in order of relative importance.

Principles for Records Creators

(C1) Digital objects must have a stable content and a fixed documentary form to be considered records and to be capable of being preserved over time. (P5)

The InterPARES Project has defined a record as "a document made or received in the course of a practical activity as an instrument or a by-product of such activity, and set aside for action or reference,"[10] adopting the traditional archival definition. This definition implies that, to be considered as a record, a digital object generated by the creator must first be a document; that is, must have stable content and fixed documentary form. Only digital objects possessing both are capable of serving the record's memorial function.

The concept of *stable content* is self-explanatory, as it simply refers to the fact that the data and the information in the record (i.e., the message the record is intended to convey) are unchanged and unchangeable. This implies that data or information cannot be overwritten, altered, deleted or added to. Thus, if one has a system that contains fluid, ever-changing data or information, one has no records in such a system until one decides to make one and to save it with its unalterable content.

The concept of *fixed form* is more complex. A digital object has a fixed form when its binary content is stored so that the message it conveys can be rendered with the same documentary presentation it had on the screen when first saved. Because the same documentary presentation of a record can be produced by a variety of digital formats or presentations,[11] fixed form does not imply that the bitstreams must remain intact over time. It is possible to change the way a record is contained in a computer file without changing the record; for example, if a digital object generated in '.doc' format is later saved in '.pdf' format, the way it manifests itself on the screen—its documentary presentation, or "documentary form"—has not changed, so one can say that the object has a fixed form.

One can also produce digital information that can take several different documentary forms. This means that the same content can be presented on the screen in several different ways, the various types of graphs available in spreadsheet software being one example. In this case, each presentation of such a digital object in the limited series of possibilities allowed by the system is to be considered as a different view of the same record having stable content and fixed form.

In addition, one has to consider the concept of "bounded variability," which refers to changes to the form and/or content of a digital record that are limited and controlled by fixed rules, so that the same query, request or interaction always generates the same result.[12] In such cases, variations in the record's form and content are either caused by technology, such as different operating systems or applications used to access the document, or by the intention of the author or writer of the document. Where content is concerned, the same query will always return the same subset, while, as mentioned, its presentation might vary within an allowed range, such as

[10] See InterPARES 2 Terminology Database, op. cit.

[11] Digital format is defined as "The byte-serialized encoding of a digital object that defines the syntactic and semantic rules for the mapping from an information model to a byte stream and the inverse mapping from that byte stream back to the original information model" (InterPARES 2 Terminology Database, op. cit.). In most contexts, digital format is used interchangeably with digital file-related concepts such as file format, file wrapper, file encoding, etc. However, there are some contexts, "such as the network transport of formatted content streams or consideration of content streams at a level of granularity finer than that of an entire file, where specific reference to "file" is inappropriate" (Stephen L. Abrams (2005), "Establishing a Global Digital Format Registry," *Library Trends* 54(1): 126. Available at http://muse.jhu.edu/demo/library_trends/v054/54.1abrams.pdf).

[12] See Duranti and Thibodeau, "The Concept of Record," op. cit.

image magnification. In consideration of the fact that what causes these variations also limits them, they are not considered to be violations of the requirements of stable content and fixed form.

Organizations should establish criteria for determining which digital objects need to be maintained as records and what methods should be employed to fix their form and content if they are fluid when generated. The criteria should be based on business needs but should respect as well the requirements of legal, administrative and historical accountability.

(C2) Record creation procedures should ensure that digital components of records can be separately maintained and reassembled over time. (P4)

Every digital record is composed of one or more digital components. A digital component is a digital object that is part of one or more digital records, including any metadata necessary to order, structure or manifest content, and that requires a given preservation action. For example, an e-mail that includes a picture and a digital signature will have at least four digital components (the header, the text, the picture and the digital signature). Reports with attachments in different formats will consist of more than one digital component, whereas a report with its attachments saved in one PDF file will consist of only one digital component. Although digital components are each stored separately, each digital component exists in a specific relationship to the other digital components that make up the record.

Preservation of digital records requires that all the digital components of a record be consistently identified, linked and stored in a way that they can be retrieved and reconstituted into a record having the same documentary presentation it manifested when last closed. Each digital component requires one or more specific methods for decoding the bitstream and for presenting it for use over time. The bitstream can be altered, as a result of conversion for example, as long as it continues to be able to fulfil its original role in the reproduction of the record. All digital components must be able to work together after they are altered; therefore, all changes need to be assessed by the creator for the effects they may have on the record.

Organizations should establish policies and procedures that stipulate the identification of digital components at the creation stage and that ensure they can be maintained, transmitted, reproduced, upgraded and reassembled over time.

(C3) Record creation and maintenance requirements should be formulated in terms of the purposes the records are to fulfil, rather than in terms of the available or chosen record-making or recordkeeping technologies. (P6)

Digital records rely, by definition, on computer technology and any instance of a record exists within a specific technological environment. For this reason, it may seem useful to establish record creation and maintenance requirements in terms of the technological characteristics of the records or the technological applications in which the records may reside. However, not only do technologies change, sometimes very frequently, but they are also governed by proprietary considerations established and modified at will by their developers. Both these factors can significantly affect the accessibility of records over time. For these reasons, references to specific technologies should not be included in records policies, strategies and standards governing the creation and maintenance of an organization's records. Only the business requirements and obligations that the records are designed to support should be explicitly kept in consideration at such a high regulatory level. At the level of implementation,

the characteristics of specific technologies should be taken into account to support the established business requirement and make possible its realization.

Technological solutions to record creation and maintenance are dynamic, meaning that they will evolve as the technology evolves. New technologies will enable new ways of creating records that meet an organization's business requirements. The rapid adoption of Web technologies to support business communication and transaction illustrates this. Specific activities for maintaining records will therefore require continuing adaptation to new situations drawing on expertise from a number of disciplines. To extend the example of the use of Web technologies, organizations creating and maintaining transactional records in a mainframe environment need to draw on knowledge of the new Web technologies from both connectivity (i.e., how to connect the mainframe to the Web) and security standpoints (i.e., how to protect the records from remote, Web-based attacks). As new technologies are used to create records, reference to new archival knowledge will continue to be required.

Technological solutions need to be specific to be effective. Although the general theory and methodology of digital preservation applies to all digital records, the maintenance solutions for different types of records require different methods. Therefore, they should be based on the specific juridical-administrative context in which the records are created and maintained, the mandate, mission or goals of their creator, the functions and activities in which the records participate and the technologies employed in their creation to ensure the best solutions are adopted for their maintenance.

Record policies that are expressed in terms of business requirements rather than technologies will need to be periodically updated as the organization's business requirements change, rather than as the technology changes. It is the role of a specific action plan to identify appropriate technological solutions for the maintenance of specific aggregations of records. The identified solutions must be monitored with regard to the possible need for modifying and updating. This requires the records creating body to be aware of new research developments in the archival and records management fields and to collaborate with interdisciplinary efforts to develop appropriate methods for the management of digital records.

(C4) Record creation and maintenance policies, strategies and standards should address the issues of record reliability, accuracy and authenticity expressly and separately. (P2)

In the management of digital records, reliability, accuracy and authenticity are three vital considerations for any organization that wishes to sustain its business competitiveness and to comply with legislative and regulatory requirements. These considerations should be directly and separately addressed in records policies and promulgated throughout the organization. The concept of reliability refers to the authority and trustworthiness of a record as a representation of the fact(s) it is about; that is, to its ability to stand for what it speaks of. In other words, reliability is the trustworthiness of a record's content. It can be inferred from two things: the degree of completeness of a record's documentary form and the degree of control exercised over the procedure (or workflow) in the course of which the record is generated. Reliability is then exclusively linked to a record's authorship and is the sole responsibility of the individual or organization that makes the record. Because, by definition, the content of a reliable record is trustworthy, and trustworthy content is, in turn, predicated on accurate data, it follows that a reliable record is also an accurate record.

An accurate record is one that contains correct, precise and exact data. Accuracy of a record may also indicate the absoluteness of the data it reports or its perfect or exclusive pertinence to

the matter in question. The accuracy of a record is assumed when the record is created and used in the course of business processes to carry out business functions, based on the assumption that inaccurate records harm business interests. However, when records are transmitted across systems, refreshed, converted or migrated for continuous use, or the technology in which the record resides is upgraded, the data contained in the record must be verified to ensure their accuracy was not harmed by technical or human errors occurring in the transmission or transformation processes. The accuracy of the data must also be verified when records are created by importing data from other records systems. This verification of accuracy is the responsibility of the physical or juridical person receiving the data; however, such person is not responsible for the correctness of the data value, for which the sending person is accountable. Thus, the receiving person should issue a disclaimer regarding accuracy of records using other persons' data.

The concept of authenticity refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted. In other words, authenticity is the trustworthiness of a record as a record. An authentic record is as reliable and accurate as it was when first generated. Authenticity depends upon the record's transmission and the manner of its maintenance and custody. Authenticity is maintained and verifiable by maintaining the identity and integrity of a record. The identity of a record is established and maintained by indicating at a minimum the names of the persons participating in the creation of the record (e.g., author, addressee); the action or matter to which the record pertains; the date(s) of compilation, filing or transmission; the record's documentary form; the record's digital presentation (or format); the relationship of the record to other records through a classification code or a naming convention; and the existence of attachments. The integrity of a record is established and maintained by identifying the responsibility for the record through time by naming the handling person or office(s)[13] and the trusted records officer[14] or the recordkeeping office,[15] identifying access privileges[16] and access restrictions[17] and indicating any annotations or any modifications (technical or otherwise) made to the record by the persons having access to it.

Thus, record reliability is a quality that is established when a record is created and implies accuracy of the data contained in the record, while record accuracy and authenticity are qualities that are connected with the transmission and maintenance of the record. The latter are therefore the responsibility of both the records creator and any legitimate successor. Authenticity is protected and guaranteed through the adoption of methods that ensure the record is not manipulated, altered, or otherwise falsified after its creation, either during its transmission or in the course of its handling and preservation, within the recordkeeping system.[18]

[13] Handling office (or person) is defined as "The office (or officer) formally competent for carrying out the action to which the record relates or for the matter to which the record pertains" (InterPARES 2 Terminology Database, op. cit.).
[14] A trusted records officer (also called records keeper or records manager) is defined as "an individual or a unit within the creating organization who is responsible for keeping and managing the creator's records, who has no reason to alter the kept records or allow others to alter them and who is capable of implementing all of the benchmark requirements for authentic records" (Ibid.).
[15] Recordkeeping office is defined as "The office given the formal competence for designing, implementing and maintaining the creator's trusted recordkeeping system" (Ibid.).
[16] Access privileges is defined as "The authority to access a system to compile, classify, register, retrieve, annotate, read, transfer or destroy records, granted to a person, position or office within an organization or agency" (Ibid.).
[17] Access restrictions is defined as "The authority to read a record, granted to a person, position or office within an organization or agency" (Ibid.).
[18] See MacNeil et al., "Authenticity Task Force Report," op. cit.

(C5) A trusted record-making system should be used to generate records that can be presumed reliable.[19]

A trusted record-making system consists of a set of rules governing the making of records and a set of tools and mechanisms used to implement these rules. To generate reliable records, every record-making system should include in its design integrated business and documentary procedures, record metadata schemes, records forms, record-making access privileges and record-making technological requirements.

Integrated business and documentary procedures are business procedures linked to documentation procedures and to the classification system (i.e., the file management plan or taxonomy) established in the organization. This integration reinforces the control over record-making procedures: it supports the reliability of records by explicitly connecting records to the activities in which they participate and to the records organization system, thereby standardizing the procedures for creating and managing those records. The integration of business and documentary procedures also establishes the basis and central means to demonstrate ownership of and responsibility for the records. A record-making metadata scheme is a list of all metadata elements that need to be documented in the course of record-making processes for the purposes of uniquely identifying each record and enabling the maintenance of its integrity and the presumption of its authenticity. Such a scheme can also be used later to verify authenticity when questioned. Records forms are specifications of the documentary forms for the various types of records generated in the record-making system. Access privileges refer to the authority to compile, edit, annotate, read, retrieve, transfer and/or destroy records in the record-making system, granted to officers and employees by the records creator on the basis of position duties and business needs. Access privileges control access to the record-making system and are established in the course of integrating business and documentary procedures through connecting specific classes of records to the office of primary responsibility for a business function or activity. The establishment and implementation of access privileges is the most important step towards ensuring that the reliability of records can be presumed. Record-making technological requirements include the hardware and software specifications for the record-making system that have a direct impact on the documentary form of records.

(C6) A trusted recordkeeping system should be used to maintain records that can be presumed accurate and authentic. (P11, P12)

A trusted recordkeeping system consists of a set of rules governing the keeping of records and a set of tools and mechanisms used to implement these rules. Every recordkeeping system should include in its design a recordkeeping metadata scheme, a classification scheme, a retention schedule, a registration system, a recordkeeping retrieval system, recordkeeping technological requirements, recordkeeping access privileges and procedures for maintaining accurate and authentic records.

A recordkeeping metadata scheme is the list of all necessary metadata to be attached to each record to ensure its continuing identity and integrity in the recordkeeping system. A classification scheme is a plan for the systematic identification and arrangement of business activities and related records into categories according to logically structured conventions, methods and procedural rules. A retention schedule is a document specifying and authorizing the

[19] There is no corresponding Preserver Principle.

disposition of aggregations of records as identified in the classification scheme. A registration system is a method for assigning a unique identifier to each created record, linked to its identity and integrity metadata. Recordkeeping access privileges refer to the authority to classify, annotate, read, retrieve, transfer and/or destroy records in the recordkeeping system, granted to officers and employees by the records creator based on position duties and business needs. Typically, access to records for purposes of classification, transfer and destruction is given only to the trusted records officer of the organization. A recordkeeping retrieval system is a set of rules governing the searching and finding of records and/or information about records in a recordkeeping system and the tools and mechanisms used to implement these rules. Recordkeeping technological requirements include the hardware and software specifications for the recordkeeping system. The procedures for maintaining accurate and authentic records are the procedures designed to ensure that the data in the records and the identity and integrity of the records in the recordkeeping system are protected from accidental or malicious corruption or loss.

To improve efficiency and reduce the potential for human-induced error, the record-making and recordkeeping systems should be designed to automate, as much as possible, the creation of the identity and integrity metadata both at the point of records creation or modification (e.g., when migrated to a new system or file format), and whenever the aggregations to which the records belong are created or modified—every record unit should automatically inherit the metadata of the higher level in the classification at the point of creation as well as whenever there are updates to the metadata of the higher level.

A records creator should indicate in its records management policy that it is the trusted records officer's responsibility to manage the recordkeeping system. The role of the trusted records officer is analogous to that of a trusted custodian; thus, the trusted records officer should have the qualifications for a trusted custodian as stated in principle C8.

A recordkeeping system that complies with the above requirements and procedures in its design and management is capable of ensuring the accuracy and authenticity of records after their creation, since these requirements and procedures establish the maximum degree of control with regard to the maintenance and use of the records.

(C7) Preservation considerations should be embedded in all activities involved in record creation and maintenance if a creator wishes to maintain and preserve accurate and authentic records beyond its operational business needs. (P7)

The concept of the records lifecycle in archival science refers to the theory that records go through distinct phases, including creation, use and maintenance and disposition (i.e., destruction or permanent preservation).

It is essential for records creators dealing with records in digital form to understand that, differently from what is the case with traditional records, preservation is a continuous process that begins with the creation of the records. Traditionally, records are appraised for preservation at the disposition stage, when they are no longer needed for business purposes. With digital records, decisions regarding preservation must be made as close as possible to the creation stage because of the ease with which they can be manipulated and deleted or lost to technological obsolescence.

The notion that records preservation starts at the creation stage requires that preservation considerations be incorporated and manifested in the design of record-making and recordkeeping systems. Each aggregation of records appraised for preservation should be identified in

accordance with the classification scheme and records retention schedule established by the records creator, and this identification should be indicated among the records metadata. The aggregations of records so identified should be monitored throughout their lifecycle so that appraisal decisions and preservation considerations can be updated and/or modified to accommodate any possible change occurring after they are first made. To monitor and implement appraisal decisions and preservation considerations, the designated preserver should be given access to the organization's recordkeeping system. Policies and procedures should be established to facilitate constant interaction between the records creator and its designated preserver.

(C8) A trusted custodian should be designated as the preserver of the creator's records. (P1)

The designated records preserver is the entity responsible for taking physical and legal custody of and preserving[20] (i.e., protecting and ensuring continuous access to) a creator's inactive records.[21] Be it an outside organization or an in-house unit, the role of the designated preserver should be that of a *trusted custodian* for a creator's records. To be considered as a trusted custodian, the preserver must:

- act as a neutral third party; that is, demonstrate that it has no stake in the content of the records and no reason to alter records under its custody and that it will not allow anybody to alter the records either accidentally or on purpose;
- be equipped with the knowledge and skills necessary to fulfil its responsibilities, which should be acquired through formal education in records and archives administration; and
- establish a trusted preservation system that is capable of ensuring that accurate and authentic copies of the creator's records are acquired and preserved.

For as long as the records are maintained by the creator in its recordkeeping system, they are active or semi-active records,[22] although under the responsibility of a trusted records officer. A records custodian trusted by the records creator as its designated preserver should maintain records that have been removed from the recordkeeping system for long-term or indefinite preservation. This trusted custodian will establish and maintain a preservation system to receive and preserve the creator's digital records. This involves ensuring that the accuracy and authenticity of the records received from the creator are assessed and maintained. Within the context of the preservation system, the designated preserver identifies appropriate preservation strategies and procedures, drawing on expertise from various disciplines, including archival science, computer science and law. The preservation procedures are implemented within the preservation system.

Only preservers that satisfy the requirements for trusted custodian are capable of fulfilling their duties of preserving authentic records over time and enabling a presumption of authenticity of the authentic copies they make for preservation purposes.

[20] The term "preservation" is defined as "The whole of the principles, policies, rules and strategies aimed at prolonging the existence of an object by maintaining it in a condition suitable for use, either in its original format or in a more persistent format, while leaving intact the object's intellectual form" (InterPARES 2 Terminology Database, op. cit.).

[21] An inactive record is defined as "A record that is no longer used in the day-to-day course of business, but which may be kept and occasionally used for legal, historical, or operational purposes" (Ibid.).

[22] An active record is defined as "A record needed by the creator for the purpose of carrying out the action for which it was created or for frequent reference" (Ibid). A semiactive record is defined as "A record which is no longer needed for the purpose of carrying out the action for which it was created, but which is needed by the records creator for reference" (Ibid.).

(C9) All business processes that contribute to the creation and/or use of the same records should be explicitly documented. (P10)

Records created in the course of carrying out one business function or one business process are often also used in the course of conducting other business functions or processes. In cases like this, records used in separate activities may be associated only with one activity in the records creator's record-making or recordkeeping system, or with none in some central "information" system or application. This practice creates difficulties for the records creator in identifying aggregations of records for accountability purposes and for its designated preserver in conducting appraisal and preservation activities.

It is recommended that policies and procedures be established that require detailed documentation of all business functions and processes contributing to the creation and use of the same records in any records creator's application or system and an explicit linkage between each record and the related workflow. Procedural manuals with such descriptions are effective in increasing the awareness of the impact of record-making and recordkeeping on the management of an organization. A subsequent different use of records after their creation can be captured by metadata, which are also capable of tracing the contexts in which records are generated.

(C10) Third-party intellectual property rights attached to the creator's records should be explicitly identified and managed in the record-making and recordkeeping systems. (P8)

Every records creator is usually aware that the records that it creates, or which are under its control or custody, contain information covered by intellectual property legislation. However, creators should also be aware that in some cases the intellectual property rights linked to a record may belong to a party other than the author and addressee.

All intellectual property rights attached to a record need to be documented in the metadata accompanying such record at the time that it is made or received and set aside. Intellectual property issues can significantly influence the reproduction of records, which is central to the processes of refreshing, converting and migrating records for either continuous use or preservation purposes. Subject to variations among different legislative environments, reproductions of records with intellectual property rights held by third parties may violate legislation that protects such rights. These issues must be identified and addressed at the stage of designing the record-making and recordkeeping systems. In the case of records identified for long-term preservation, long-term clearance of such rights should be addressed explicitly in the creator's record policy.

(C11) Privacy rights and obligations attached to the creator's records should be explicitly identified and protected in the record-making and recordkeeping systems. (P9)

Privacy legislation protects the rights of individuals with reference to personal data that may be part of any record used and maintained by a records creator with whom they have interacted. The limits of privacy depend on the legislative framework in which the records creator operates. The framework may be in conflict with the access policy linked to the mandate of the records creator and even with the access to information legislation in the same jurisdiction.

The presence of personal information within the records should be identified and documented within the metadata schema linked to the records in the record-making and recordkeeping systems of the creator. Metadata schemas that note and administer the use of personal

information contained within the records must be embedded in record-making and recordkeeping systems. This will enable the protection of personal information through the establishment of system-wide access privileges. In cases where records are to be preserved indefinitely, privacy issues relating to access to records must be expressly resolved (i.e., explicit permissions must be sought from the individuals concerned), ideally prior to record creation. This is the best way to ensure that the records are managed in accordance with privacy legislation and that the preserver will be able to effectively include the privacy issues relevant to the records in the preservation feasibility study during appraisal. The designated preserver for each records creator should, as a trusted custodian, be granted access to records containing personal information to perform preservation activities. Processing of personal information for maintenance or preservation purposes is different from the use of it for research or business purposes. Regardless of the legislative framework, the records creator should be able to demonstrate that processing of records containing personal information does not put such information at risk of unauthorized access.

Responsibility for processing records containing personal data for maintenance and preservation purposes must reside with the records creator and its legitimate successors. Although the practice of outsourcing these functions to specialized commercial operators is authorized and regulated under most existing privacy legislation, the practice should still be avoided whenever possible to minimize the number of individuals authorized to access and/or process the records, thus reducing the risk of unauthorized disclosure of personal information in the records and of jeopardizing the ability to obtain permission to process personal information for maintenance or preservation purposes.

In the case of records that are not yet designated for permanent preservation, appraisal decisions should be taken before the initial mandate for processing personal information has expired to ensure that the legal basis for retaining such records is still in force.

(C12) Procedures for sharing records across different jurisdictions should be established on the basis of the legal requirements under which the records are created. (P13)

Records creators with branches in geographically separate areas (i.e., areas that are covered by different legislation), must be aware that different access, privacy and intellectual property laws may have an impact on their records-sharing activities. Such sharing activities encompass records exchange within the records creator or with outside organizations, such as governments or business partners. This includes providing records to a trusted preserver, where the latter operates in a legal environment different from that of the records creator.

The fact that records are freely accessible in one jurisdiction does not imply that they can be accessed in the same way in other jurisdictions. Records creators must investigate such issues and address them in their policies.

(C13) Reproductions of a record made by the creator in its usual and ordinary course of business and for its purposes and use, as part of its recordkeeping activities, have the same effects as the first manifestation, and each is to be considered at any given time the record of the creator. (P3)

In the digital environment, the first manifestation of a record, be it a draft, an original or a copy, only exists when first composed in the creator's record-making system, if it is an internal record, or when first received in the creator's recordkeeping system, if it is transmitted from the

outside. When the record is closed and saved into the record-making or recordkeeping system, its first manifestation technically disappears, as the saving action decomposes it into its digital components. Any later manifestation of the digital record is a reproduction resulting from an assembly of its digital components. Conceptually, however, records creators can use any reproduction of a record's first manifestation as if it were the record's first manifestation, as long as the reproduction is made in the usual and ordinary course of carrying out business activities and used for such activities. This means that each reproduction in sequence should have the same admissibility in court as the record's first manifestation and be given the same weight.

To establish that a record is reproduced in the usual and ordinary course of business, it is necessary to set out routine procedures in writing. In effect, if reliable records have been generated in a trusted record-making system and their accuracy and authenticity have been maintained together with that of the received records in the creator's recordkeeping system, then all records should have the same authority and effects as their first manifestation.

Although, according to the theory of the record (i.e., diplomatics), an "original" record in a digital system is the first manifestation of a received record and, if after closing such manifestation the original no longer exists, it might be useful to look at three examples of statutory laws pertaining to the meaning of "original." Common to all three variations is the principle that it is the relationship of a record to the business of the creator that determines whether the record in question has the authority and effects of an original.

> Example 1: The U.S. Federal *Rules of Evidence* distinguishes between originals and duplicates, with greater value as evidence given to originals. For digital records, it is noteworthy that if "data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"[23]
>
> Example 2: The quality of being original is acknowledged in Italian legislation in terms of adding weight or greater trustworthiness to records. Italian legislation emphasizes the difference between digital data (original) and any kind of output of those data (copy), by establishing that "any data or document electronically created by any public administration represents a primary and original source of information that may be used to make copies on any kind of medium for all legal purposes."[24]
>
> Example 3: The *Electronic Signatures Law of the People's Republic of China* regards a digital record as an original if it meets the two following qualifications: it must be 1) capable of presenting the content effectively and of being retrieved and consulted at any moment, and 2) capable of unfailingly showing the integrity of the content from the moment of its completion. However, annotations made to a data electronic document [digital record] and changes of presentation occurring in the process of data exchanging, storing and displaying are not considered to affect its integrity.[25]

[23] United States House of Representatives, *Federal Rules of Evidence*, Article X. Contents of Writings, Recordings, and Photographs: Rule 1001. Definitions, Committee on the Judiciary, Committee Print No. 8 (December 31, 2004). Available at http://judiciary.house.gov/media/pdfs/printers/108th/evid2004.pdf. The same rule generalizes that "any counterpart" to the writing or recording "intended to have the same effect by a person executing or issuing it" is an original.
[24] Italy, DPR 445/2000, art. 9, par. 1. Available at http://www.parlamento.it/parlam/leggi/deleghe/00443dla.htm.
[25] China, *Electronic Signatures Law of the People's Republic of China*, art. 5. Translated by Sherry Xie. See also Sherry Xie (2005). "InterPARES 2 Project - Policy Cross-domain: Supplements to the Study of Archival Legislation in China (Report I)," 3. Available at http://www.interpares.org/display_file.cfm?doc=ip2(policy)archival_legislation_CHINA_SUPPLEMENT.pdf.

Principles for Records Preservers

(P1) A designated records preserver fulfils the role of trusted custodian. (C8)

The designated records preserver is the entity responsible for taking physical and legal custody of and preserving (i.e., protecting and ensuring continuous access to) a creator's inactive records. Be it an outside organization or an in-house unit, the role of the designated preserver should be that of a *trusted custodian* for a creator's records. To be considered as a trusted custodian, the preserver must:

- act as a neutral third party; that is, demonstrate that it has no stake in the content of the records and no reason to alter records under its custody and that it will not allow anybody to alter the records either accidentally or on purpose;
- be equipped with the knowledge and skills necessary to fulfil its responsibilities, which should be acquired through formal education in records and archives administration; and
- establish a trusted preservation system that is capable of ensuring that accurate and authentic copies of the creator's records are acquired and preserved.

The acquisition of a creator's records is undertaken by the preserver, who, after having assessed the accuracy and authenticity of the records, produces an authentic copy of them from the creator's recordkeeping system. Records that are acquired this way are authentic copies of the records of the creator identified for long-term preservation, because they are made by the designated preserver in its role of trusted custodian.

The authentic copies of the creator's records are then kept by the trusted custodian in a trusted preservation system, which should include in its design a description and a retrieval system. This trusted preservation system must also have in place rules and procedures for the ongoing production of authentic copies as the existing system becomes obsolete and the technology is upgraded. This requirement is consistent with the final recommendations of InterPARES 1, which developed the *Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records*,[26] a set of requirements to be implemented by the preserver. It should be noted that the simple fact of reproducing records in the preserver's preservation system does not make the results authentic copies; such designation must be provided by the preserver's authority.

A sustainable preservation strategy requires close collaboration between a records creator and its designated preserver as trusted custodian. It is the preserver's responsibility to take the initiative in collaborating with the creator to establish acquisition and preservation procedures and in advising the creator in any records management activities essential to the preserver's acquisition and preservation activities.

(P2) Records preservation policies, strategies and standards should address the issues of record accuracy and authenticity expressly and separately. (C4)

An accurate record is one that contains correct, precise and exact data. The accuracy of a record is assumed when the record is created and used in the course of business processes to carry out business functions, based on the assumption that inaccurate records harm business interests. However, when records are transmitted across systems, refreshed, converted or migrated for preservation purposes, or the technology in which the record resides is upgraded,

[26] See MacNeil et al., "Authenticity Task Force Report," op. cit., and, more specifically, Authenticity Task Force, "Appendix 2."

the data contained in the record must be verified to ensure their accuracy was not harmed by technical or human errors occurring in the transmission or transformation processes. This verification of accuracy is the responsibility of the preserver who carries out the transmission or transformation process; however, such person is not responsible for the correctness of the data value, for which the creator remains accountable, just as is the case for the reliability of the records containing the data.

The concept of authenticity refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted. In other words, authenticity is the trustworthiness of a record as a record. A record is authentic if it can be demonstrated that it is as it was when created. An authentic record is as reliable and accurate as it was when first generated. Authenticity depends upon the record transmission and the manner of its preservation and custody. Thus, it is a responsibility of both the records creator and its legitimate successor (i.e., either the person or organization acquiring the function(s) from which the records in question result and the records themselves, or a designated records preserver).

Authenticity is protected and is verifiable by ensuring that the identity and the integrity of a record are maintained. The identity of a record is what distinguishes it from all other records. It is declared at the moment of creation by indicating at a minimum the following attributes: the names of the persons participating in the creation of the record (e.g., author, addressee); the action or matter to which the record pertains; the date(s) of compilation, filing or transmission; the record's documentary form; the record's digital presentation (or format); the relationship of the record to other records through a classification code or a naming convention; and the existence of attachments. The record identity so declared must be maintained intact through time first by the creator and its trusted records officer while the record is in active or semi-active use, and subsequently by the designated records preserver when the record is designated as inactive. The integrity of a record is its wholeness and soundness and can only be inferred from circumstantial evidence related to the person who held responsibility for the record through time, from access privileges and access restrictions and from the indication of any annotation or modification (technical or otherwise) that such person(s) with access to record might have made to it. Thus, the establishment and maintenance of record integrity are supported by declaring the following record attributes: the names of the handling office(s), the office of primary responsibility[27] for the record over time and/or the recordkeeping office and the designated preserver; the access privileges code[28] and the access restriction code;[29] and the list of annotations[30] and of format changes.[31]

Authenticity is not a quality that can be bestowed on records after their creation and maintenance by any preservation process. A preserver can only protect and maintain what was transferred under its responsibility. Authenticity is protected and maintained through the adoption of methods that ensure that the record is not manipulated, altered, or otherwise falsified after its transfer. It is the preserver's responsibility to assess the authenticity of records considered for acquisition into a preservation system and to ensure that it remains intact after the

[27] Office of primary responsibility is defined as "The office given the formal competence for maintaining the authoritative version or copy of records belonging to a given class within a classification scheme" (InterPARES 2 Terminology Database, op. cit.).
[28] Access privileges code is defined as "The indication of the person, position or office authorized to annotate a record, delete it, or remove it from the system" (Ibid.).
[29] Access restriction code is defined as "The indication of the person, position or office authorized to read a record" (Ibid.).
[30] List of annotations is defined as "Recorded information about additions made to a record after it has been created" (Ibid.).
[31] List of format changes is defined as "Recorded Information about modifications to a record's documentary form or digital format after it has been created" (Ibid.).

transfer to such system by respecting within the preserving unit or organization the same *Benchmark Requirements* that bind the creator (e.g., access privileges, measure against corruption or loss) and the *Baseline Requirements* for preservers.

(P3) Reproductions of a creator's records made for purposes of preservation by their trusted custodian are to be considered authentic copies of the creator's records. (C13)

Reproductions of digital records in the creator's record-making and recordkeeping systems made in the usual and ordinary course of activity for either action or reference purposes can be considered to have the same authority and effects as the first manifestation of the same records. Reproductions of a creator's records for preservation purposes rather than in response to a creator's business need are considered authentic copies of the records of the creator, because they are never used in their present manifestation for action or reference by the creator itself. The creator's records and their authentic preservation copies are the same records but at different phases in their lifecycle and thus at a different status of transmission.[32] The former are used by their creator to achieve business goals, while the latter are made by the preservers for preservation purposes.

Copies of records in the preserver's preservation system may not be designated authentic if the preserver has made them for purposes other than preservation; for example, a copy from which personal identifiers are removed may be made for access purposes. Ultimately, only the preserver has the authority to designate a copy as authentic.

(P4) Records preservation procedures should ensure that the digital components of records can be separately preserved and reassembled over time. (C2)

Every digital record is composed of one or more digital components. A digital component is a digital object that is part of one or more digital records, including any metadata necessary to order, structure or manifest content and that requires a given preservation action. For example, an e-mail that includes a picture and a digital signature will have at least four digital components (the header, the text, the picture and the digital signature). Reports with attachments in different formats will consist of more than one digital component, whereas a report with its attachments saved in one PDF file will consist of only one digital component. Although digital components are each stored separately, each digital component exists in a specific relationship to the other digital components that make up the record.

Preservation of digital records requires that all the digital components of a record be consistently identified, linked and stored in a way that they can be retrieved and reconstituted into a record having the same presentation it manifested when last closed. Each digital component requires one or more specific methods for decoding the bitstream and for presenting it for use over time. The bitstream can be altered, as a result of conversion, for example, as long as it continues to be able to fulfil its original role in the reproduction of the record. All digital components must be able to work together after they are altered; therefore, all changes need to be assessed by the preserver for the effects they may have on the record.

[32] In diplomatics, the status of transmission is the degree of perfection of record. There are three possible statuses of transmission: draft, original and copy. Copies are than further categorized according to their authority, and the most authoritative among the copies is the authentic copy; that is, a reproduction that is declared conforming to the reproduced entity by an officer having the authority to do so. Professional archivists are among such officers.

The preserver must be prepared to advise the creator, directly or through development of recommended standards, on the types of digital components that the preserver's system is able to sustain. Where standards governing the types and formats of digital components are common to both the record-making and recordkeeping systems and the record preservation system, the preserver can directly influence the creator towards those standards that will facilitate meeting the preservation requirements. Where no common standards exist or can reasonably be adopted, the preserver must understand the degree of interoperability of certain types and formats of digital components. This understanding will provide a basis for the preserver to assess the capability of the preservation system to preserve the digital components and their relationships as they emerge from the creator's record-making and recordkeeping systems.

Highly interoperable formats—that is, formats that are not tied to specific applications or versions of applications—are generally seen to provide a better basis for preservation work. It is important, however, not to focus exclusively on the interoperability of formats at the expense of the relationships between them that also must be preserved. For example, an HTML-based Web page may be comprised of digital components that are highly interoperable, but the version of HTML coding used to structure the components may be an old version with many deprecated terms (i.e., terms that are not recognized by current software browsers that may be used to reproduce the Web page).

(P5) Authentic copies should be made for preservation purposes only from the creator's records; that is, from digital objects that have a stable content and a fixed documentary form. (C1)

A record is defined by InterPARES, following the traditional archival definition, as "a document made or received in the course of a practical activity as an instrument or a by-product of such activity and set aside for action or reference."[33] This definition implies that, to be considered as a record, a digital object generated by the creator must first be a document; that is, must have stable content and fixed documentary form. Only digital objects possessing both are capable of serving the record's memorial function.

The concept of *stable content* is self-explanatory, as it simply refers to the fact that the data and the information in the record (i.e., the message the record is intended to convey) are unchanged and unchangeable. This implies that data or information cannot be overwritten, altered, deleted or added to. Thus, if one has a system that contains fluid, ever-changing data or information, one has no records in such a system until one decides to make one and to save it with its unalterable content.

The concept of *fixed form* is more complex. A digital object has a fixed form when its binary content is stored so that the message it conveys can be rendered with the same documentary presentation it had on the screen when first saved. Because the same documentary presentation of a record can be produced by a variety of digital presentations, fixed form does not imply that the bitstreams must remain intact over time. It is possible to change the way a record is contained in a computer file without changing the record; for example, if a digital object generated in '.doc' format is later saved in '.pdf' format, the way it manifests itself on the screen—its documentary presentation, or "documentary form"—has not changed, so one can say that the object has a fixed form.

[33] See the InterPARES 2 Terminology Database, op. cit.

One can also produce digital information that can take several different documentary forms. This means that the same content can be presented on the screen in several different ways, the various types of graphs available in spreadsheet software being one example. In this case, each presentation of such a digital object in the limited series of possibilities allowed by the system is to be considered as a different view of the same record having stable content and fixed form.

In addition, one has to consider the concept of "bounded variability,"[34] which refers to changes to the form and/or content of a digital record that are limited and controlled by fixed rules, so that the same query, request or interaction always generates the same result. In such cases, variations in the record's form and content are either caused by technology, such as different operating systems or applications used to access the document, or by the intention of the author or writer of the document. Where content is concerned, while, as mentioned, the same query will always return the same subset, its presentation might vary within an allowed range, such as image magnification. In consideration of the fact that what causes these variations also limits them, they are not considered to be violations of the requirements of stable content and fixed form.

Based on this understanding, any preservation policy should clearly state that reproductions of authentic copies for preservation purposes can only be made from the creator's records, as identified by the creator.[35]

The preserver should know (or help establish) the creator's criteria for identifying the digital objects that are maintained as records and the methods employed to stabilize their content and fix their form. This is consistent with the preserver's responsibility to advise the creator on its record creation processes and technologies. This advising activity will also provide the preserver with the critical information needed to understand the business activities and processes that caused the records to come into being and with the ability to assess their continuing identity and integrity.

(P6) Preservation requirements should be articulated in terms of the purpose or desired outcome of preservation, rather than in terms of the specific technologies available. (C3)

Digital records rely, by definition, on computer technology, and any instance of a record exists within a specific technological environment. For this reason, it may seem useful to establish record preservation requirements in terms of the technological characteristics of the records or the technological applications in which the records may reside. However, not only do technologies change, sometimes very frequently, but they also are governed by proprietary considerations established and modified at will by their developers. Both these factors can significantly affect the continued accessibility of digital records over time. For these reasons, references to specific technologies should not be included in preservation policies and standards. Only the requirements and obligations that the records are designed to support should be explicit within record preservation policies and standards. It is only at the level of implementation that specific technologies should, indeed must, be named.

Technological solutions to record preservation issues are dynamic, meaning that they will evolve as the technology evolves. This affects record preservation in two ways. First, it makes it possible to adopt new strategies to meet preservation needs, as happened with the use of XML to support the long-term preservation of structured records. Second, it creates opportunities for drawing on expertise from a number of disciplines. These two issues are interconnected. Thus,

[34] See Duranti and Thibodeau, "The Concept of Record," op. cit.
[35] See principle C1 in the Principles for Creators regarding the identification of records.

for example, while utilization of XML is, by itself, only one activity for preservation, it might be matched with using data grid technology as a stable and enduring platform to support XML-based records. By experimenting with these combinations, new archival knowledge will continue to be both acquired and required.

Technological solutions also need to be specific to be effective. Although the general theory and methodology of digital preservation applies to all digital records, the preservation solutions for different types of records require different methods. These should be based on the specific context in which the records are created and maintained, the functions and activities to which the records are linked and the technologies employed for record-making and recordkeeping to ensure the best solutions are designed for preserving each type of record.

Preservation policies that are expressed in terms of record requirements rather than technologies will be more stable, needing updates only if the record requirements change, rather than as the technology changes. Preservation action plans will likely need to be updated more frequently to identify appropriate technological solutions for the digital preservation of specific aggregations of records. The identified solutions must be monitored with regard to the possible need for modifying and updating.

(P7) Preservation considerations should be embedded in all activities involved in each phase of the records lifecycle if their continuing authentic existence over the long term is to be ensured. (C7)

The concept of the records lifecycle in archival science refers to the theory that records go through distinct phases, including creation, use and maintenance and disposition (destruction or permanent preservation).

It is essential for preservers who acquire digital records to understand that, differently from what is the case with traditional records, preservation is a continuous process that begins with the creation of the records. Analogue records are appraised for preservation at the disposition stage, when they are no longer needed by the creator for business purposes. With digital records, decisions relevant to preservation must be made as close as possible to the creation stage because of the ease and the speed with which digital objects can be manipulated, deleted by accident or on purpose, or lost to technological obsolescence.

The notion that records preservation starts at the creation stage requires that preservation considerations be incorporated and manifested in the design of record-making and recordkeeping systems. Each aggregation of records appraised for preservation should be identified in accordance with the classification scheme and the records retention schedule established by the records creator in collaboration with the preserver, and this identification should be indicated in the records metadata. The records so identified should be monitored throughout their lifecycle by the preserver, so that appraisal decisions and preservation considerations can be updated to accommodate any possible changes occurring after they are first made. Appraisal decisions need to be reviewed to ensure that the information about the appraised records is still valid, that changes to the records and their context have not adversely affected their identity or integrity and that the details of the process of carrying out disposition are still workable and applicable to the records. To monitor and implement appraisal decisions and preservation considerations, the designated preserver should obtain continuing access to the records creator's recordkeeping system within limits agreed upon with the creator and reflected in the preserver's access privileges. The preserver should establish procedures to facilitate constant interaction with the records creator.

(P8) Third-party intellectual property rights attached to the creator's records should be explicitly identified and managed in the preservation system. (C10)

Preservers know that records under records creators' control usually contain information covered by intellectual property legislation. They should also be aware that, in some cases, the intellectual property rights attached to records belong to a party other than the author; that is, the intellectual property rights reside with a third party. Third-party intellectual property rights should be documented in the metadata accompanying such records because they influence the processes of refreshing, converting and migrating them for either continuous use or preservation purposes. Subject to variations in different legislative environments, reproductions of records with third-party intellectual property rights attached to them may violate legislation that protects such rights. In the case of records identified for long-term preservation, long-term clearance of such rights should be addressed explicitly with the records creator.

Because preservation in a digital environment involves making copies, intellectual property rights have become an issue, not just for access as in the past, but for preservation. It is the preserver's responsibility; first, to advise the creator on how to address intellectual property issues in its record-making and recordkeeping systems, and, second, to ensure that intellectual property issues are addressed in the design of the preservation system. In particular, any issues relevant to third-party intellectual property rights should be cleared before the transfer of records to be preserved from the creator to the preserver. The latter must consider these issues as a part of the assessment of feasibility of preservation.

(P9) Privacy rights and obligations attached to the creator's records should be explicitly identified and protected in the preservation system. (C11)

Privacy legislation protects the rights of individuals with reference to personal data that may be part of any record used and maintained by a records creator with whom they have interacted. The limits of privacy depend on the legislative framework in which the records creator operates. It may be in conflict with the access policy linked to the mandate of the records creator and even with the access to information legislation in the same jurisdiction. Besides lobbying for exceptions, the designated preserver should ensure that the consequences of the existing situation for preservation and access are clearly understood.

The presence of personal information within the records should be identified and documented among the metadata linked to the records in the record-making and recordkeeping systems of the creators. This is the best way to ensure that the records are managed in accordance with privacy legislation and that the preserver will be able to effectively include the privacy issues relevant to the records in the preservation feasibility study during appraisal. The designated preserver for each creator should, as a trusted custodian, obtain access to records containing personal information to perform preservation activities. Archival processing of personal information for preservation purposes is different from the use of it for research or business purposes. Regardless of the legislative framework, the creator and the preserver should be able to demonstrate that archival processing of records containing personal information does not put such information at risk of unauthorized access.

Preservers should also insist that responsibility for processing records containing personal data for preservation purposes must reside with the records creator and its legitimate successors. Although the practice of outsourcing these preservation functions to specialized commercial operators may be authorized and regulated under most existing privacy legislation, the practice

should still be avoided whenever possible to minimize the number of individuals authorized to access and/or process the records, thus reducing the risk of unauthorized disclosure of personal information in the records and of jeopardizing the ability to obtain permission to process personal information for preservation purposes.

In the case of records that are not yet designated for permanent preservation, appraisal decisions should be taken before the initial mandate for processing personal information has expired to ensure that the legal basis for retaining such records is still in force.

(P10) Archival appraisal should identify and analyze all the business processes that contribute to the creation and/or use of the same records. (C9)

A record may be created for one purpose and then subsequently used for different purposes by different persons. Any appraisal decision should consider all uses of the record and be aware of the business processes behind them. This is necessary to make an informed decision about what to preserve as well as to be able to dispose effectively of all possible copies of the records that have not been selected for preservation.

The use of records or information within records by different business processes may be desirable from the creator's standpoint in terms of providing a degree of interoperability among the creator's information and record systems. In such situations, the preserver should advise the creator that metadata attached to records used by many business processes must identify each relevant business process. This is critical for the creator because it ensures the authenticity of the records by establishing their identity and integrity in each context. It is also critical for the preserver who must understand all contexts in which the records were used to effectively undertake appraisal and also to meet the baseline requirements for maintaining authenticity for any records acquired into the preservation system.

(P11) Archival appraisal should assess the authenticity of the records. (C6)

Appraisal decisions should be made by compiling information about kept records and their context(s), assessing their value and determining the feasibility of their preservation.[36]

As part of the assessment of value, preservers must establish the grounds for presuming that the records being appraised are authentic. This means that preservers must ensure that each record identity has been documented and maintained as documented and must ascertain the degree to which the records' creator has guaranteed their integrity by making sure that its records are intact and uncorrupted. The evidence supporting the presumption of authenticity must be measured against the InterPARES *Benchmark Requirements*.[37]

(P12) Archival description should be used as a collective authentication of the records in an archival fonds. (C6)

Archival description of a fonds emerges from the comprehensive analysis of the various relationships interwoven in the course of the formation and accumulation of records and therefore is the most reliable means of establishing the continued authenticity of a body of

[36] See Terry Eastwood et al., "Part Two – Choosing to Preserve: The Selection of Electronic Records: Appraisal Task Force Report," in Duranti, *Long-term Preservation*, op. cit., 67–98. Online reprint available at http://www.interpares.org/book/interpares_book_e_part2.pdf.

[37] See the already cited benchmark requirements in MacNeil et al., "Appraisal Task Force Report," op. cit.

interrelated records. While the authenticity of individual records can be in part established through their metadata, the authenticity of aggregations of records (i.e., file, series or fonds), can only be proved through archival description.

It has always been the function, either explicit or implicit, of archival description to authenticate the records by perpetuating their administrative and documentary relationships; but, with digital records, this function has moved to the forefront. In fact, as original digital records disappear and an interminable chain of non-identical reproductions follows them, the researchers looking at the last of those reproductions will not find in it any information regarding provenance, authority, context or authenticity.

The authentication function of archival description is different from that of a certificate of authenticity, because it is not simply an attestation of the authenticity of individual records, but a collective attestation of the authenticity of the records of a fonds and of all their interrelationships as made explicit by their administrative, custodial and technological history (including a description of the recordkeeping system(s) within which they have been maintained and used), the scope and content and the hierarchical representation of the records aggregates. It is also different both from the identity and integrity metadata attached to individual records, which are part of the record itself and are reproduced time after time with it and from the additional metadata attached to records aggregations (e.g., file, series) within the recordkeeping system to identify them and document their technological transformations.

The unique function of archival description is to provide an historical view of the records and of their becoming, while presenting them as a universality in which each member's individuality is subject to the bond of a common provenance and destination.

(P13) Procedures for providing access to records created in one jurisdiction to users in other jurisdictions should be established on the basis of the legal environment in which the records were created. (C13)

Different jurisdictions may have different laws and regulations with regard to access rights in relation to the protection of privacy, intellectual property and any other kind of public or private interests (e.g., market sensitive records). Preservers who are a unit of a records creator (e.g., in-house archival programs or archives) that has geographically separated branches falling under different legislation must be aware of the impact of such diverse legal contexts on their records-sharing activities. This will affect access policies relevant to both internal and external sharing activities.