Principles and Criteria

Principles are statements that have general validity in a given sector or field. In applied sciences, they are conceptual statements on which a science, an argument, or a reasoning is based, derived from the observation of individual facts. Criteria are the norms on which distinctions are based, judgements are made, and different lines of action or conduct are decided.

The extensive and in-depth investigations of the InterPARES project over three years have been distilled into a set of fourteen principles and corresponding criteria for the development of policies, strategies, and standards.

Any records preservation policy, strategy, or standard should:

Principle	Criteria
1. address records specifically rather than digital objects generally; that is, it should address documents made or received and set aside in the course of practical activity.	A record is distinguished from other digital objects by virtue of the fact that it possesses a fixed documentary form, a stable content, an archival bond with other records, and an identifiable context. It participates in or supports an action and at least three persons are involved in its creation (i.e., an author, a writer, and an addressee).[i]
2. focus on authentic electronic records.	An authentic electronic record is one that is what it claims to be and that is free from tampering or corruption. Accordingly, proving the authenticity of an electronic record involves establishing its identity and demonstrating its integrity on the basis of the benchmark and baseline requirements for authenticity. The identity of a record refers to the distinguishing character of a record, that is, the attributes of a record that uniquely characterize it and distinguish it from other records. The integrity of a record refers to its wholeness and soundness: a record has integrity when it is complete and uncorrupted in all its essential respects. This does not mean that the record must be precisely the same as it was when first created for its integrity to exist and be demonstrated. When we refer to an electronic record, we consider it essentially complete and uncorrupted if the message that it is meant to communicate in order to achieve its purpose is unaltered.[ii]
3. recognize and provide for the fact that authenticity is most at risk when records are transmitted across space (i.e., when sent between persons, systems, or applications) or time (i.e., either when they are stored offline, or when the hardware or software used to process, communicate, or maintain them is upgraded or replaced).	Assertions that electronic records are more susceptible to tampering and corruption than traditional, hard-copy records need to be placed in context. While threats to the integrity of electronic records undoubtedly exist, digital information technology offers possibilities for very strong protection of their integrity. These possibilities are strongest within the confines of a specific system. For example, it is possible to track every access to a records system and every action on any record in the system. A system can be designed so that, once filed, a record is never out of file: users get access only to copies of the record. System design can also preclude any alteration or destruction of

	records except by authorized persons. Simple procedures such as redundant storage and regular back-up can also make it easy to recover from any inappropriate alteration or deletion. However, such controls are only effective within the confines of a system. When a record is taken out of a system, or when the system itself is modified, systematic control is at risk.[iii]
4. recognize that preservation of authentic electronic records is a continuous process that begins with the process of records creation and whose purpose is to transmit authentic records across time and space.	This process is defined as "chain of preservation," that is, a system of controls that extends over the entire life cycle of records and ensures their identity and integrity in any action that affects the way the records are represented in storage or presented for use. The benchmark requirements for assessing the authenticity of the creator's electronic records define evidence that demonstrates how the records creator established and maintained the chain of preservation while the records remained in its custody. The baseline requirements supporting the production of authentic copies of electronic records articulate what the preserver must do to ensure that the chain remains unbroken from the moment the records are transferred to the archives.[iv]
5. be based on the concept of trust in records keeping and record preservation and specifically on the concepts of a trusted record-keeping system and the role of the preserver as a trusted custodian.	Records should be made and maintained in a trusted record-keeping system and preserved by a trusted custodian. A trusted record-keeping system comprises the whole of the rules that control the creation, maintenance, and use of the records of the creator and that provide a circumstantial probability of the authenticity of the records within the system. To be considered a trusted custodian, the preserver must demonstrate that it has no reason to alter the preserved records or allow others to alter them, and is capable of implementing all of the baseline requirements.[v]
6. be predicated on the understanding that it is not possible to preserve an electronic record as a stored physical object: it is only possible to preserve the ability to reproduce the record.	Reproducing an electronic record means to be able to render it with the content and any required elements of documentary form and annotations that such record possessed before reproduction.[vi]
7. recognize that the physical and intellectual components of an electronic record do not necessarily coincide and that the concept of digital component is distinct from the concept of element of documentary form.	A digital component is distinguished from an element of documentary form on the basis of the fact that a digital component is a digital object that contains all or part of the content of an electronic record, and/or data or metadata necessary to order, structure, or manifest the content, and that requires specific methods for preservation. In contrast, extrinsic and intrinsic elements of form are those characteristics of a record that constitute its external appearance and convey the action in which it participates and the immediate context in which it was created.[vii]

8. specify the requirements a copy of a record should satisfy to be considered equivalent to an original.	In principle, an original electronic record is the first complete and effective record. However, in an electronic environment, no original survives. Every faithful copy of such a record's content and of its documentary form is to be considered a copy in the form of the original, which is equivalent to the original as to its consequences. Any kind of copy that is declared authentic by an officer entrusted with such a responsibility is also equivalent to the original.[viii]
9. integrate records appraisal in the continuous process of preservation.	Records should be selected for long-term preservation on the basis of their continuing value, assessment of their authenticity, and the feasibility of their preservation.[ix]
10. integrate archival description in the continuous process of preservation.	Archival description should serve as a collective attestation of the authenticity of the records and their relationships in the context of the fonds to which the records belong in conformance with the baseline requirements.[x]
11. explicitly state that the entire process of preservation must be thoroughly documented as a primary means for protecting and assessing authenticity over the long term.	To support the assertion of the authenticity of preserved electronic records, the preserver should document, at a minimum: the records creator's practices to support a presumption of authenticity, in accordance with the benchmark requirements for authenticity; and the processes of bringing the records into the archives and maintaining them over time, and the reproduction of records, in accordance with the baseline requirements for the production of authentic copies of records.[xi]
12. explicitly recognize that the traditional principle that all records relied upon in the usual and ordinary course of business can be presumed to be authentic needs to be supplemented in the case of electronic records by evidence that the records have not been inappropriately altered.	In addition to the evidence that they were created and used in the usual and ordinary course of business, records should be presumed authentic on the basis of the criteria listed as benchmark requirements in the "Authenticity Task Force Report" or verified authentic by the preserver.[xii]
13. recognize that the preserver is concerned with both the assessment and the maintenance of the authenticity of electronic records. The assessment of the authenticity of electronic records takes place before records are transferred to the custody of the preserver as part of the process of appraisal, while the maintenance of the authenticity of copies of electronic records takes place once they have been transferred to the preserver's custody as part of the process of long-term preservation.	The assessment of the authenticity of electronic records should be based on the benchmark requirements, while the maintenance of the authenticity of copies of electronic records should be based on the baseline requirements.[xiii]
14. draw a clear distinction between the preservation of the authenticity of records and the authentication of a record.	Authentication is a declaration of a record's authenticity at a specific moment in time by a juridical person entrusted with the authority to make such declaration. It takes the form of an authoritative statement, which may be in the form of words or symbols, that is added to or inserted in the record attesting that the record is authentic.

	Digital signatures—which identify the sender of a data object and verify that it has not been altered in transmission—can support the authentication of electronic records, but they are not sufficient to establish the identity and demonstrate the integrity of an electronic record over the long term.[xiv]

[i] See "Authenticity Task Force Report"..

[ii] See "Authenticity Task Force Report".

[iii] See Appendix 2; "Preservation Task Force Report".

[iv] See Appendix 2.

[v] See "Authenticity Task Force Report".

[vi] See "Authenticity Task Force Report"; "Preservation Task Force Report".

[vii] See "Preservation Task Force Report".

[viii] See "Preservation Task Force Report"; "Authenticity Task Force Report".

[ix] See "Appraisal Task Force Report".

[x] See "Authenticity Task Force Report".

[xi] See Appendix 2; "Appraisal Task Force Report"; "Preservation Task Force Report".

[xii] See "Authenticity Task Force Report"; "Appraisal Task Force Report".

[xiii] See Appendix 2.

[xiv] See "Authenticity Task Force Report".