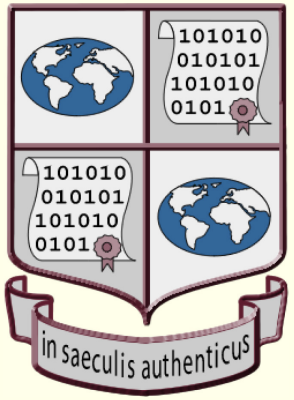
InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems



Making and Maintaining Digital Materials

Guidelines for Individuals

Purpose, Scope & Structure

- Purpose: to help individuals and small groups to make informed decisions
- Scope: from selection of hardware and software to provisions for long-term preservation
- Structure:
  - an introduction stating the issues and defining the terms;
  - ten recommendations, each followed by an explanatory narrative;
  - conclusion.

Introduction

- Issues:
  - accessibility, readability, intelligibility, compatibility, interoperability
  - proliferation of copies, identification of the final or official version
  - risks for intellectual property rights, accuracy and authenticity
  - vulnerability to viruses and technology failure
  - technological obsolescence
  - inconsistency of hybrid record systems
- Definitions:
  - record, publication, document, information, data
  - reliability, accuracy, authenticity, authentication

1. Selecting Software & Hardware

- Choose software that presents materials as they originally appeared
- Choose software & hardware that allow you to share materials easily
- Use software that adheres to standards
- Maintain the specifications of software
- Document changes when software is customized
- Document the construction of your system

2. Ensuring Stability of Digital Materials

- Stability is the essential characteristic of every document and means:
  - fixed content (content cannot be overwritten, altered, deleted or expanded) and
  - fixed documentary form (the rules governing its presentation are unchangeable and the possibilities are limited)

- The documentary form of each record associated with each activity should be defined at the outset.

3. Identifying Digital Materials

- Record essential information about the record so that it may be uniquely identified (identity metadata):
  - names of author, writer, originator, addressee
  - name of action, matter, subject, or simply the title
  - dates of compilation, transmission, receipt, filing
  - documentary form
  - digital presentation (format, wrapper, encoding, etc)
  - attachments, if applicable
  - intellectual rights, if applicable
  - presence or removal of digital signature, or other form of authentication
  - name of person responsible for the record, if applicable
  - name of or code for the file or group of records in which the record belongs
- Distinguish different versions of the record and identify the official version among its identity metadata

4. Supporting the Presumption of Integrity

Record information that helps to infer that the record is the same as when created (integrity metadata):

- name(s) of handling persons over time
- name of person primarily responsible for keeping the record
- indication of additions (annotations) made to the record
- indication of technical changes (e.g. format, encoding, upgrading, changes to digital components, migration)
- Indication of presence or removal of digital signature
- planned removal from the system, transfer to a custodian, deletion
- existence and location of duplicates outside the system

5. Organizing Materials into Logical Groupings

- Separate records from other types of materials
- Create a classification scheme or filing plan or a structured directory to provide a logical place for each record
- Ensure that such scheme, plan or directory corresponds to the way your non-digital records are organized
- Provide each new digital record with an identifier showing its proper place in the scheme (e.g. a code or the name of the file and of the higher groups in which the file belongs) and include this among the record's identity metadata
- Identify how long records need to be kept
- Make decisions at the group or file level, not the individual record (maintaining consistency between the records on different media belonging to the same file or group)

6. Using Authentication Techniques

- Nature of authentication techniques
  - digital signature
- Obsolescence and authentication
  - preservation issues
- Managing documents with digital signatures
  - integrity metadata

7. Protecting Your Materials from Unauthorized Action

- You must be able to demonstrate that it is impossible to tamper with your materials without being identified
- Restrict physical access to your computer(s)
- Create access permissions for all legitimate users of your system
- Maintain an audit trail of access to your system and the materials in it
- If you cannot prove the authenticity of your material, it is irrelevant that it is authentic

8. Protect Records from Accidental Loss & Corruption

- Ensure that your system is backed up at least once a day
- Choose and implement the best backup technique for your situation
- The backup system should include an audit trail
- The purpose of your backup tapes or discs is to recover the system in case of failure, not to keep records. Destroy your backups on a regular basis (e.g., every third day)
- Duplicates of your material should be kept on additional hard drives. If they are kept outside the system on tapes or discs, remember to refresh and upgrade them periodically

9. Protecting Materials Against Hardware & Software Obsolescence

- Eliminate dependence on specific hardware
- Transfer hardware functionality to software
- Plan for regular technology upgrades (keeping in mind the need for backward compatibility)
- Consider external storage for infrequently used records (including computer output microfilm for textual records that do not require random search)
- If you remove materials from your live system, associate with it the system documentation and all the necessary information about the material to be able to maintain accessibility and to understand the material itself

10. Planning for Long-Term Preservation

- Identify the materials that need to be preserved for the long term
- Identify a trusted custodian for the records (in-house or external)
- Establish a preservation strategy early and in consultation with the designated trusted custodian
- Follow this set of recommendations

Conclusion

- Be aware of the risks of neglecting to manage your digital materials properly
- Adopt measures that work best in your situation
- Consult with professional archivists
- Review other InterPARES documents (including its bibliographies)