Model Digital Preservation Policy

Table of Contents

Go back to Table of Contents

Executive Summary

March 2022. Version 1.0
Contributors: ***Corey Davis, Corinne Guimont, Grant Hurley, Jeremy Morse, James Phillpotts, Michelle Polchow, Jennifer Regala, Heather Staines, Willa Tavernier, Alicia Wise, and Melina Zavala***

As the digital scholarly record grows in size, volume, and complexity, the stakeholders responsible for stewarding this information into the future must develop plans, strategies, and activities to ensure that these materials remain available and usable for as long as they are needed. These stakeholders include publishers (whether free-standing or based in academic institutions) of materials for which long-term availability is essential to the advancement of collective knowledge. Stakeholders also include the organizations that provide the network of contextual metadata, data, software, standards, and other materials linked to these publications.

Policy frameworks — as expressed by these guidelines developed by the NASIG Digital Preservation Policy Working Group — can help publishing organizations articulate the scope, activities, and principles that support the digital preservation of materials in their care. The size, type, needs, and resources of publishing organizations will vary considerably. However, all share a responsibility for ensuring that the materials they publish are available for current and future use. They also share a responsibility for communicating their preservation policies and practices to authors, customers, readers, and users. Having an explicit digital preservation policy helps to ensure that preservation activities are repeatable, visible, and transparent to stakeholders. Critically, this includes transparency regarding what an organization is, and is not, preserving.

Core to the work of digital preservation is the ability to keep digital objects authentic and reliable into the future; work which includes maintenance and management strategies that adapt to new risks and technologies as they arise. Conducting these activities consistently and sustainably over many years requires coordination from different stakeholders, including creators, selectors, user communities, and units across an organization. Policies can help organize these manifold activities and provide support for the financial, technical, and human resources required over time. This work can be complex, and the policy of an organization might include that some aspects of this are addressed through arrangements with expert third parties, which might include national libraries or digital preservation services, such as those provided by CLOCKSS or Portico.

The Model Digital Preservation Policy guidelines are envisioned as a resource for publishing organizations to adapt to their specific contexts and needs. Created from a survey of digital preservation policies in use across many different types of scholarly publishing organizations, each section includes an explanation of its purpose alongside sample text or a section guide that can be adapted for different preservation contexts. The model policy is intended to fulfill the

role of a policy *framework* or *strategy* that connects the mission and mandate of an organization to the work of digital preservation by identifying the scope, strategies, principles, roles and responsibilities of its preservation program. The guidelines conclude with a glossary of key terms used throughout the document.

The policy guidelines were developed by the NASIG Model Digital Preservation Policy Working Group in 2020-2022. The project was undertaken under the auspices of the NASIG Digital Preservation Committee after a survey of member institutions expressed a need for more guidance and resources for writing digital preservation policies. Members of the group were recruited from stakeholder organizations, including the Library Publishing Coalition and the Society for Scholarly Publishing, as a joint effort to build capacity and resources for the preservation of scholarly publications.

How to Use This Document

The size, type, needs, and resources of organizations involved in publishing activities that would benefit from having a digital preservation policy vary considerably. This document is intended to provide a guide to writing a policy that will fit the needs of your organization. In many instances, sample text is provided. In other cases, where the content of a particular section will vary widely depending on the type of organization (see *Scope* and *Related Documents*), the Working Group considered that a section guide on what might be included or a list of suggestions would be more practical.

It is expected that organizations will want and need to tailor the model policy to fit their specific circumstances. Sections that are clearly relevant should be included, but will not be applicable in all cases. For example, where an organization is working with expert third-party digital preservation providers, it may be desirable to provide links out to their documentation, rather than duplicating this document. Where sample text is provided in the model policy, this should only be adopted when it is relevant to or desired by the specific organization, and there is no need to use the exact language given. The samples are not an exhaustive representation of the types of statements that could be used by an organization for this section of their policy. “The organization” or a derivation of that term is used as a placeholder for the name of the institution adapting these statements for its own use.

Go back to Table of Contents

Introduction

Central to digital preservation are a commitment of resources over the long term, and continuous decision making. The introductory section identifies the rationale for developing and sustaining a digital preservation program, including its purpose, mandate, and objectives. Including this information helps formalize the strategic role of digital preservation activities at your organization and the rationale for committing ongoing resources to these activities.

The first part of the introduction will typically include:

- *The date that the policy is made and the date of any updates*
- *A general description of the organization*
- *A broad description of the digital resources that will be covered by the policy*
- *The institutional unit(s) responsible for preparing, approving, and updating the policy.*

Additional subsections of the introduction provide space for articulating the organization's strategic purpose, commitments, and goals:

- *Purpose: Identifies the reason(s) why the organization preserves content. The "Purpose" section makes your organization's commitment to its digital preservation program and stakeholders direct and explicit. It identifies the importance of digital preservation to the organization and makes a direct link between this and the policy as a mechanism for supporting and driving this program of work. It may also include identifying the resources the organization will commit (time, attention, active management, money, technological resources).*

- *Mandate: Identifies the source of your organization's commitment to building and sustaining a digital preservation program. Ideally, this subsection would point towards external organization-wide strategic planning, mission/mandate statements, or other institutional, contractual, or legal obligations that establish its preservation mandate.*

- *Objectives: Establishes the broad goals and aims of the organization's digital preservation program: what are the intended outcomes and benefits? How do these activities support the broader strategic goals of the organization? Stated objectives should be high-level rather than identifying specific processes: reserve identification of specific functions to the "Preservation Activities" section below.*

Go back to Table of Contents

Sample Text

Date:
Updated:

This statement outlines the preservation policy of [*name of organization*], [*organization type, e.g. a not-for-profit open-access publisher in the social sciences and humanities with a strong focus on research in cultural studies, political economy, and social change around the globe*]. This policy covers [*type of digital resources the policy covers e.g. version of record content published by the organization, including research articles, book chapters, and case reports in online resources*], plus related metadata and supplementary materials.

This policy was created and will be monitored and managed by [*e.g. an interdepartmental standing committee on digital preservation*]*, and has been approved by our* [*e.g. board, department head, etc.*].

Purpose

Our organization is committed to the long-term preservation of the scholarly work that we publish in recognition of the fact that current authors and customers, as well as future researchers, will need access to the work we publish today and that this requires a coordinated effort on the part of the various actors involved in scholarly publishing.

The Digital Preservation Policy formalizes the organization's commitment to the stewardship of the scholarly work we publish and establishes digital preservation as core to our operations. The purpose of the policy is to present a shared understanding of how digital preservation activities will be applied, managed, and sustained across the organization and to support ongoing resource allocation, decision-making, communication, and collaboration in the development and sustainability of our digital preservation program.

Mandate

As outlined in our Mission Statement, the organization publishes [*e.g. leading research in social sciences and humanities*]. We make a commitment to authors, peer reviewers, librarians, and readers to ensure continued access to the published record over time. The preservation of our published scholarly materials fulfills our contractual obligations with authors, which specify that materials will be archived and made accessible in perpetuity. We also maintain a contractual relationship with CLOCKSS to deposit material for preservation on a regular basis and these arrangements are reported transparently through the Keepers Registry.

Objectives

The organization will:

Sources:

"National Library of Australia Digital Preservation Policy 4th Edition", 2013.
"Digital Preservation Policy", Indiana University Libraries, March 2017.

"ACS Knowledgebase", ACS Central Science.

- Define the designated community or communities that the organization serves to ensure our preservation and access program continues to meet the needs of our user community and other stakeholders
- Identify the scope of materials to be preserved and the associated preservation activities to be employed for each class of material in scope
- Assign roles and responsibilities for the digital preservation activities identified to staff members at the organization
- Adopt and contribute to community-supported standards and collaborative partnerships for digital preservation
- Fulfill the requirements of all contracts, licenses, and agreements related to retention, preservation, and access
- Develop and assess the digital preservation program in response to the organization’s needs and via feedback from authors, librarians, and other stakeholders.

Go back to Table of Contents

Principles

This section identifies the broad concepts and functions that guide a digital preservation program and activities. The principles should guide decision-making and support the organization's more granular policies, action plans, and procedures, and the assessment and benchmarking of the program. Adherence to standards such as OAIS, NDSA Levels of Preservation, or METS/PREMIS may also be confirmed in this section.

The principles can be represented as a single block, or be broken down into foundational principles, which address the more theoretical or values-based aspects of the program, and operational principles, which address the functional aspects of the program and link to other documents such as repository-level policies, procedures, and content action plans.

Section Guide

Common elements of principles statements are:

- Organizational commitment
  - A statement referring to the organization's mission or mandate and commitment to the preservation of its collections
  - Statements pointing to a framework for organizational governance and decision-making around digital preservation activities, including:
    - Ensuring roles and responsibilities for digital preservation work will be defined and assigned
    - How decision-making around the distribution of resources for digital preservation activities will be informed.

- Conformance with internal and external policies, procedures, standards, and frameworks
  - An indication that the organization's digital preservation activities will adhere to:

Sources:

"UVic Libraries digital preservation framework", University of Victoria, March 2017.

"SFU Library Digital Preservation Framework," Simon Fraser University.
"Digital Preservation Services," University of Alberta, 2021-04-19.

"Digital Preservation Management," Simon Fraser University Archives

■ Internal sources: the organization's governance and organizational structure, policies and procedures, internal standards, and contracts and agreements ■ External sources: legislation, standards, and community practices ○ Commitments to ensuring consultation and communication with internal and external stakeholders, including possibly making information about digital preservation activities transparent or available for auditing and quality-assurance purposes. ● Digital preservation values: ○ Statements referring to key principles to help guide the digital preservation program and decision-making: ■ An explanation of the value that digital preservation activities bring to the organization ■ Endorsement of high-level strategies such as risk management and mitigation, preservation monitoring, and content action plans. This could link to specific activities as defined in the "Strategy" section above ■ Indication that metadata is in scope for preservation in addition to digital objects themselves ○ Statements indicating commitment to collaboration, research, and development in the field. The following sample text is not an exhaustive representation of the types of principles that could be endorsed by an organization for this section of their policy.	and Records Management Department, May 2017.

Sample Text

Foundational Principles

- The organization's digital preservation strategies are directed by our mandate to build, steward, and preserve our collections on behalf of our user community.
- The digital preservation program will comply with the organization's existing policies, procedures, and/or relevant applicable legislation.
- We affirm that the purpose of digital preservation is to maintain the long-term availability of digital assets over time.
- Digital preservation is not a binary state where digital assets are preserved or not. It is a property of the policies and procedures used to manage digital assets that either increase or diminish their usefulness over time.
- The preservation of metadata, including descriptive, technical, and administrative metadata, using community-developed standards whenever possible, is as important as the preservation of the digital objects themselves.
- We recognize that continuous, meaningful engagement with our designated community is vital to ensuring the accessibility and usability of our digital assets.

Operating Principles

- A central component of the organization's digital preservation strategy is risk identification and mitigation. Policies, action plans, and/or procedures will be defined and documented for content groups in order to guide strategic actions and identify and mitigate risks to digital assets.
- Responsibility for preservation actions is clearly defined and assigned to units within the organization and systematically implemented and documented.
- The organization will obtain sufficient control, both physical and intellectual, as required for long-term preservation and access activities, and maintain a record of these controls. This includes adherence to all applicable contracts, licenses, and agreements, and includes rights to migrate files to new formats over time.

- Digital preservation programs at the organization seek technologically, organizationally, and financially sustainable solutions, including through collaboration and cooperation with external organizations and collaborative networks where appropriate.
- The organization will demonstrate leadership and support development in the digital preservation field within its financial and staff resources by:
    - Using open-source software
    - Contributing to standards creation
    - Participating in scholarly and practical discussion
    - Developing tools and technologies
- The organization will ensure stewardship of institutional knowledge of digital preservation by:
    - Providing training for staff
    - Documenting procedures
    - Maintaining and disseminating resource lists within the organization
- The organization will document and share, where possible, its digital preservation policies. procedures, and actions for internal review, peer review, and public dissemination for the purposes of transparency and accountability to its user community.
- The organization will react to organizational, environmental, and technological change, positive or negative. Policies, action plans, and/or procedures will be subject to periodic review to adjust priorities and evaluate effectiveness.
- The organization will use persistent identifiers such as DOIs, ISBNs, ORCiDs, RORs, etc.
- The organization will prioritize the use of platforms and tools from which preserved objects and all associated metadata can be extracted with integrity.

Go back to Table of Contents

Scope

When defining scope, it is worth considering two categories of materials separately, as the requirements and activities are likely to be different:

- *Materials that a user community will access directly*
- *Materials that are intended to be accessed by specific stakeholders (e.g. staff), such as would enable the re-creation, maintenance, or management of user-accessed materials.*

Sample text for General Principles *and a Section Guide for* What We Preserve*,* What We Don't Preserve*, and* Selection Criteria *are set out below.*

Sample Text

General Principles

The primary focus of our digital preservation activities is on preserving the intellectual content of the materials acquired, ingested, and published in our systems. However, preservation always entails making choices about what to preserve. In the interest of transparency, the selective application of preservation practice should be the result of a deliberate decision-making process, the results of which are delineated in our preservation policy. Defining the scope of the policy includes what materials are covered under the policy, but also what aspects of a publication; policies that discuss preservation only in terms of discrete digital files may not address the complexity of enhanced digital publications, for example.

Sources:

"Digital Repository Services Digital Preservation Policy," University of Michigan Library, July 2020.

"U-M Registered Formats and Service Levels," University of Michigan Library.

Section Guide

What We Preserve

For end-user access

It is recommended that this section focuses on defining the "Version of Record" of a digital publication and what its constituent parts are, including related metadata and supplementary materials. For example, if the Version of Record is defined as including everything essential to understanding and supporting the scholarly argument of a work, then it becomes easier to identify what needs to be included in the scope of a preservation policy that keeps that work useful over time.

Example materials to consider for inclusion:

- Journal content (research articles, reviews, etc.)
- Institutional collections
- Texts (ebooks, articles, dissertations, etc.)
- Embedded assets (images, videos, etc.)
- Metadata
    - Descriptive
    - Administrative, including Intellectual Property Rights
    - Technical
- Relationships among the parts
- Datasets
- Annotations or comments
- Peer review notes (open or proprietary) and author responses
- Previous versions (e.g. pre-prints)
- Externally hosted supplementary content (e.g. datasets)
- Material omitted from print versions (e.g. additional tables or figures)
- Annotations
- Comments
- Journal front matter (e.g. editorial information, policies)
- Related blog/social media posts or other promotional material

Where applicable, the policy should address the management of preservation masters and access derivatives, whether they are managed similarly or differently.

"UVic Libraries digital preservation framework," University of Victoria, March 2017.

Other aspects of a publication may be considered essential for certain enhanced digital publications (particularly in the digital humanities):

- Look and feel
- Navigation elements (if essential for understanding the relationships among the parts)
- Custom software

When preservation in its current form requires higher-cost solutions (e.g. emulation) that may be prohibitive, you may consider creating a static record of its current implementation using web archiving tools. Such a process entails creating a new document (e.g. a WARC file of a crawled website) which is then subject to your preservation policies. Some web archiving methods (such as LOCKSS) only capture certain parts of a website (e.g. HTML and PDFs from a subset of web pages) rather than attempting to archive the entire site. This distinction should be articulated in your policy.

For stakeholder access

Most preservation policies do not cover this material explicitly, leaving it to desktop or server support to maintain access through a backup-restore policy. If you intend to include this material explicitly in a preservation policy, it is best to consider the metadata, packaging, and discovery needs of such materials so they can fulfill their intended purpose.

Example materials:

- Contracts, memoranda of understanding, rights agreements, and any other documentation of rights and commitments pertaining to publication and preservation
- Internal assets
- Products of publishing work
- Supporting documents compiled during research
- Production archive/previous versions that went through the review and revision process
- Reviewer notes (for non-open peer review) and author responses
- Accepted manuscripts
- Peer-reviewed manuscripts (post-prints)

Special consideration:

- Look and feel
  - Even where this isn't preserved in the access layer, consider the value of keeping a consistent internal record of UI design evolution over the life of the content.
- Software
  - Thinking of the delivery systems themselves, rather than published software objects. Open Source delivery systems admittedly blur this distinction.

Section Guide

What We Don’t Preserve

Anything considered above that has been ruled out, even in selected circumstances, should be described here, preferably with some account of the reasoning behind the decision. Doing this is in the interest of transparency for external users and stakeholders (so they have a clearer idea of what to expect when accessing these resources in the future) and in the interest of clarity for internal stakeholders during their decision-making processes while performing preservation tasks (to remove ambiguity about what is covered under the policy).

Section Guide

Selection Criteria

Each institution, or perhaps each service within an institution, will have its own criteria for determining what content is in or out of scope for its preservation program. Criteria to consider include:

- Mission of the institution
- Importance of the content to user communities
- Quality of the digital resource
- Uniqueness of the digital resource
- Risk to the items/collections

Open Access content should be subject to the same preservation policy and practice as controlled content, and therefore access should not be a consideration in preservation selection criteria.

Go back to Table of Contents

Preservation Activities

Preservation activities are the procedures, tools, and techniques used to implement this policy.

Sample Text

This section identifies the key activities required to sustain the value of our digital content. Responsibility for decision-making and delivery of strategies lies with [*name position or group*]. Collaboration with [*name positions or groups*] is necessary to ensure effective implementation of these strategies.

Integrity

The following strategies will be used to ensure the authenticity of objects and preservation activities:

- Validity. The object's chain of custody and provenance, starting as early as possible but at the very least from the time it entered our preservation systems. This information is necessary in order to understand the history of the object and to denote any transformations or changes that have occurred to the content: for example, any updates, errata, corrections, or retractions.
- Representation. Information on the object's representation. For every digital object, some level of interpretation is necessary in order to transform the object from binary data into something that humans can interpret.
- Fixity information. We will keep sufficient metadata on the object to ensure that, at any point in the future, the object remains in a complete, unaltered, authentic, and uncorrupted state. We will employ fixity checks as appropriate to ensure the integrity of files.

Methods

We may employ various strategies for preserving the above properties such as:

- Refreshing
- Digital archaeology/forensics
- Bit preservation
- Migration
- Web archiving
- Emulation

Sources:

"Strategic Framework for Digital Preservation", Digital Archive, McMaster University Library.

"Policy for Preservation of Digital Resources", Columbia University Libraries.

"UVic Libraries digital preservation framework", University of Victoria, March 2017.

Morse, Jeremy. "Preservation Policies and Why Every Publisher Needs One," LPF 2018 Preservation Panel, 2018.

"Sustaining The Value: The British Library Digital Preservation Strategy 2017-2020", The British Library, January 2017.

"Digital Preservation Framework", University of Minnesota, 2014.

And such other additional strategies as may emerge in the future.

Monitoring

- We will monitor formats (at both the file level and the metadata level) used in our systems in order to ensure their suitability for long-term preservation.
- We will participate actively, where appropriate and feasible, in research, development, and implementation of new practices for the preservation of digital resources.

Storage and Security

All systems in the digital preservation infrastructure will meet or exceed [*name of organization*] policies for information security and related procedures, appendices, and standards. These policies are available at [*link*] *OR*
Where digital preservation infrastructure is provided by a third-party organization, we will ensure that the organization's recovery strategy complies with our minimum standards for cybersecurity.

Recovery

Our recovery strategy is built on redundancy and multiple modes of recovery. Where digital preservation infrastructure is provided by a third-party organization, we will ensure that the organization's recovery strategy complies with this provision.

Access

Access for the public: Members of the public can access all published content as well as [*descriptive, administrative, and structural*] metadata.
OR

Access to published content is limited to [*active subscribers/ institutional account holders*].

Access for creators: Creators of content stored in our systems will be able to access all publicly accessible content [and pre-prints and post-prints for up to 10 years after submission].

Access to the following types of content is restricted to [*other types of stakeholders e.g. staff*]:

- *List restricted content here*
- *See Scope>>What We Preserve>>Stakeholder Access>>Example Materials*

Access to the following types of content is mediated and available only by request [*e.g. because it is held in a dark archive or in a non-real time-access medium, such as tape backup or Amazon Glacie*r]:

- *List restricted content here*
- *See Scope>>What We Preserve>>Stakeholder Access>>Example Materials above.*

Management

- We will develop and publish selection guidelines setting out the criteria for long-term retention of digital assets.
- We may develop tiers of preservation services based on selection guidelines. Each of these tiers may have its own retention period.

  For examples of selection guidelines see Scope>>Selection Criteria above.
- We may outsource preservation activities to third-party vendors or consortial arrangements where these meet the requirements of this policy.
- We will follow any best practices published by [*insert professional, regional, national, or international agency*] so far as it is feasible, and provide public documentation of any departure from these best practices.

Go back to Table of Contents

Roles and Responsibilities

This section details who is involved (positions, not individuals), at what level they are involved, and who is charged with preservation responsibilities. In addition to any monetary commitments, human resources are real resources, so this cost should be factored as part of the total cost of a publishing program (Open Access or otherwise), regardless of funding sources.

The people involved in preservation can vary depending on the structure of your organization. Presses or publishing units within a library may have different sets of resources from those that are organizationally separate from the library, and from commercial publishers. Larger publishers may have more resources and more teams in dedicated roles than smaller publishers. Institutions of any size may choose to outsource the entire infrastructure for preservation to a third-party provider. Despite this, in all cases, selection decisions must be made. Preservation planning should include (as much as possible) those with information and technology, preservation, and metadata knowledge or expertise. Organizations that do not already have this support in place should assess preservation needs and commit budget and staff where possible.

In order to fulfill the commitments made elsewhere in your policy, you must allocate sufficient resources to fulfill those preservation functions. Those resources should be described in this section.

Sample Text with Section Guide

Decisions on what will be preserved are made by [*individual positions, departments, or committees*] in consultation with:

- Information and technology support
  (*Whether within the publishing department, the library, or at the university level, IT support can be crucial for implementing and maintaining preservation systems*)
- Preservation experts
  (*If available, preservation experts within the publishing staff, library, or university can assist in determining best practices and policies for various pieces of content held within the publishing department or press*)
- Metadata coordinators
  (*Those with a deep knowledge of descriptive and technical metadata within the publishing department, library, or university should be involved in creating standards and schemas for preservation*)
- Repository managers
  (*In cases where content is stored or pushed to an institutional repository, repository managers should be consulted about existing policies for the repository and how those may or may not affect your preservation policy*)
- Library acquisitions/subject specialists
  (*Acquisitions and subject specialists in your library, regardless of whether or not the publishing department falls within the library, may help identify the need for preservation for some specialized content*)
- Copyright/licensing experts
  (*Copyright and licensing experts can identify what can and cannot legally be preserved and at what level of access. These individuals should still be consulted when the content is openly licensed.*)

Decision-making also takes into consideration the needs and interests of authors, reviewers, and editors who provide the different pieces of content and information that may be needed for preservation.

The publishing team (who may consult or collaborate with those identified above) is responsible for undertaking digital preservation activities. These may include:

- Selecting and managing content for preservation
- Promoting and implementing good practices
- Actively monitoring technology and workflows
- Responding to technological obsolescence through migration or other strategies

Sources:

"UVic Libraries digital preservation framework," University of Victoria, March 2017.

"ICPSR Digital Preservation Policy Framework," ICPSR.

"Cornell University Library Digital Preservation Policy Framework," Cornell University.

"Digital Preservation Policy," Dartmouth College Library.

"PURR Digital Preservation Policy," Purdue University Research Repository, April 2012.

- Collaborating with other institutions on possible shared services and activities focused on digital preservation
- Reviewing this document as needed based on the agreed-upon review cycle.

Collaboration

This section provides a statement of commitment to cooperation or collaboration within the organization or with like organizations, which "acknowledges that the organization's effort exceeds or will exceed available resources and may not guarantee the safety of all vital assets" (McGovern). A statement of commitment to collaboration could also be included in the "Principles" section.

Sample Text

We collaborate to advance our preservation strategy, and are keen to continuously learn from others. This includes collaborating and learning from partners internally and externally.

McGovern, Nancy. "Digital Preservation Management Model Document," Digital Preservation Management Workshops and Tutorial, September 2014.

Go back to Table of Contents

Framework Administration and Review Cycle

This section identifies details about the creation and maintenance of the policy.

Such details might include the date the document was approved or changed (if not recorded elsewhere in the policy such as in header information), who approved it, and the date it was made effective. Additional details should identify how frequently the policy will be reviewed and updated, and who at the organization is responsible for initiating this review, which might be a specific role or a committee or working group.

Sample Text

The framework was approved and made effective on March 1, 2021, by the Director of Operations.

This document will be reviewed and updated as needed with a full review every [*x number of years*] to align with changes in technology, preservation strategies, and/or expertise. The review process will be initiated by the Digital Preservation Working Group.

Go back to Table of Contents

Related Documents

This section links to other institutional documentation that supports digital preservation work at the organization.

Section Guide

Examples might include such documentation as

- Disaster plan
- Records management policy
- Collections development policy
- Sensitive data policy
- Other institutional policies
- Other industry level policies/standards

Sources:

"Digital Preservation Policy", Indiana University Libraries, March 2017.

"Cornell University Library Digital Preservation Policy Framework", Cornell University.

Glossary

A glossary provides concise explanations of key concepts and definitions of institutionally specific terms and acronyms used throughout the policy. The glossary should be specific to the contents of the policy; any terms that you think would require definition for your intended audience should be included here, and any not used in the policy can be removed.

Sample Text

Authenticity: the quality of digital materials being what they purport to be and free from tampering or corruption. Authenticity is composed of identity and integrity (establishing that materials remain complete and unaltered over time).	The InterPARES 2 Project
Bit preservation: a preservation approach that uses periodic checksum validation of digital objects to ensure they have not been modified or corrupted. This approach may also include "maintaining onsite and offsite backup copies, virus checking, … and periodic refreshment to new storage media", but does not include a broader commitment to ensuring materials are accessible and therefore may not align with an organization's definition of "digital preservation."	Glossary - Digital Preservation Handbook

Checksum: a method of verifying the integrity of digital files, commonly used for the monitoring of a file's fixity over time. Checksums are often called a "digital fingerprint" because the checksum algorithm provides a unique alphanumeric string for a particular manifestation of a file. If a file's contents are modified in any way, re-calculating the file's checksum will provide a different alphanumeric string. This allows for the continuous monitoring of fixity, as well as the identification of duplicate files.	Concepts - Scholars Portal
Designated community: a group of primary users that the preserving institution has identified as able to access and understand the preserved information without expert assistance. This means that an appropriate level of contextual information must be preserved alongside the materials themselves. Note that multiple designated communities are possible and that they may change over time.	Glossary - Digital Preservation Handbook; Brian Lavoie, The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition, 2014)
Digital archaeology/forensics: includes methods and procedures to rescue content from damaged media or from obsolete or damaged hardware and software environments using specialized techniques.	Digital Preservation Strategies | Digital Preservation Management
Digital preservation: "the series of managed activities necessary to ensure continued access to digital materials for as long as necessary" (DPC). Digital preservation combines policies, strategies, and actions to ensure the accurate rendering of authenticated content over time, regardless of the challenges of media failure and technological change. Digital preservation applies to both born-digital and reformatted content.	Glossary - Digital Preservation Handbook
Digital object: an aggregation of one or more individual files and/or bitstreams designated as the subject of digital preservation actions and activities. For example, a journal article composed of XML full text plus a series of PNG figures is a digital object; a single PDF containing the same information would also be a digital object.	
Emulation: "a means of overcoming technological obsolescence of hardware and software by developing techniques for imitating obsolete systems on future generations of computers."	Glossary - Digital Preservation Handbook
Identity: technical, administrative, descriptive, and other metadata that uniquely identifies the digital materials from others.	The InterPARES 2 Project

Information security: the practice of protecting the integrity and privacy of data, both in storage and in transit.	What is Cyber Security? | Definition, Types, and User Protection | Kaspersky
Integrity: establishing that a file remains complete and unaltered over time. One method of doing so is using checksums. Part of authenticity.	The InterPARES 2 Project
Metadata: commonly defined as “data about data.” Metadata is information describing the significant aspects of a resource that adds contextual information to that resource to aid in its discovery and management. In the context of digital preservation, descriptive metadata enables access to resources stored in preservation systems. For example, DublinCore or JATS metadata may be used for descriptive purposes to record information about a resource in order to provide context and information about its provenance. In the case of a journal article, this would be information like article authors, title, and persistent identifiers. Technical metadata such as fixity information via checksums and file format identifications assists in the preservation of a resource over time. And administrative metadata such as rights information enables determinations around access and other preservation events that may be undertaken by the preserving institution.	Glossary - Digital Preservation Handbook
METS: stands for *Metadata Encoding and Transmission Standard*. This XML standard is maintained by the Library of Congress as a container for metadata about digital objects. It is commonly used for digital preservation purposes to structure and encode preservation-supporting descriptive, administrative, and technical metadata in combination with PREMIS metadata.	Metadata Encoding and Transmission Standard (METS) Official Web Site
Migration: “a means of overcoming technological obsolescence by transferring digital resources from one hardware/software generation to the next. The purpose of migration is to preserve the intellectual content of digital objects and to retain the ability for clients to retrieve, display, and otherwise use them in the face of constantly changing technology.”	https://www.dpconline.org/handbook/glossary#D
NDSA Levels of Preservation: a resource designed for digital preservation practitioners to aid in designing and assessing digital preservation program activities. The *Levels* define four levels of preservation across five functional areas: storage, integrity, control, metadata, and content.	NDSA Levels of Digital Preservation
OAIS: stands for *Open Archival Information System*. OAIS is a reference model, produced by the Consultative Committee for Space Data Systems starting in 1995 with input from the library and archives community, for defining the broad concepts, functional components, and responsibilities required to preserve information over time. The OAIS standard was formalized as an ISO standard 14721 in 2002 with a revision in 2012. An OAIS-type archive consists “of an organization, which may be part of a larger organization, of people and systems, that has	Glossary - Digital Preservation Handbook Brian Lavoie, *The Open Archival Information*

accepted the responsibility to preserve information and make it available for a Designated Community. It meets a set of responsibilities, as defined in section 4 of the OAIS standard."	*System (OAIS) Reference Model: Introductory guide* (2nd Edition, 2014)
PREMIS: stands for *Preservation Metadata: Implementation Strategies*. Maintained by the Library of Congress and the PREMIS Editorial Committee, PREMIS is the key standard for structuring and storing digital preservation metadata. PREMIS entities include information about digital objects, agents, events, rights, and environments.	http://www.loc.gov/standards/premis/
Refreshing: transferring from one digital medium to another, including identical media, at regular intervals, while monitoring and maintaining integrity, to avoid data loss that can be caused by physical deterioration.	The InterPARES 2 Project
Stakeholders: Internal stakeholders are the individuals and units within an organization tasked with identifying their organization's past, existing, and future content and then creating a digital preservation strategy and executing its implementation. These internal stakeholders include, for example, content creators, selectors, and curators; developers; platform administrators; and anyone who solicits, maintains, stores, and will ultimately partner in preserving the organization's content. External stakeholders are those individuals and groups who are not directly attached to an organization by employment, membership, studentship, or other such connection. In some cases they may be impacted by the organization's content but do not share in the responsibility for collecting it, hosting it, or preserving it. However, they are interested in and impacted by the longevity and future availability of this content. Such external stakeholders include but are not limited to end-users, user communities, readers, authors, librarians, members, students, historians, and any other interested parties who are sustained in any way by the organization's content.	
User community: see "Designated community."	
WARC: The Web ARChive format is a container format for archived websites, also known as ISO 28500:2009. It is a revision of the Internet Archive's ARC file format used to store web crawls harvested from the World Wide Web.	Glossary - Digital Preservation Handbook