

Version 2.0 Digital Preservation Policy Framework: Outline

Prepared by Nancy Y. McGovern, Digital Preservation Officer, ICPSR
January 2007 (last revised October 2007)

Overview

This document provides an outline for constructing the digital preservation policy framework for ICPSR and offers a step towards identifying core components of a digital preservation policy framework to encourage a community standard for digital preservation policy documents. The outline was developed to produce a digital preservation policy framework that:

- Addresses the seven attributes of a Trusted Digital Repository
- Presents the high-level perspective of an organization's digital preservation program
- Reflects current not future capabilities of the digital preservation program
- Provides links to documents containing more detailed and frequently-updated documents, e.g., lower level policies and procedures
- Points to the digital preservation plan for near-term priorities and timeframes
- Documents the policy approval and maintenance process

The framework includes one section for each of the seven attributes of a trusted digital repository: OAIS compliance, administrative responsibility, organizational viability, financial sustainability, technological and procedural accountability, system security, and procedural accountability. Some sections contain more than one component.

Framework Components

OAIS Compliance: consists of an explicit statement of the intent of the digital preservation program to comply with the Open Archival Information System (OAIS) Reference Model approved as ISO 14721 in 2003. The digital preservation plan delineates the specifics of OAIS compliance and the self-assessment results for the digital preservation program documents the status of the program's OAIS compliance. **Links:** strategic plan, preservation plan

Administrative Responsibility: makes an explicit commitment to digital preservation and to compliance with prevailing standards and practice.

Purpose: makes explicit the intentions of an institution and defines the essential role a digital preservation program plays in fulfilling the mission to protect the organization's digital assets. This section defines the rationale for the framework, identifies responsible parties and stakeholders, indicates the intended audience for the document, and places the document in the context of organization-wide efforts. The purpose statement might range from broad to narrow, reflecting the variations in intention for different types of digital archives. **Links:** mission statement, high-level policy statements, strategic plans.

Mandate: stipulates the authority, jurisdiction, or governance upon which responsible parties have developed the digital preservation program, e.g., laws, legislation, policies, and mission. This section may also address requirements that are not specifically identified as preservation, e.g., legal admissibility, authenticity, FOIA, ADA, Data Protection Acts, copyright legislation, public records acts, E-Government, National Grid

for Learning (UK). *Links*: laws, legislation, contracts, policies, mission statement, regulations.

Objectives: states the high-level aims and targets of the organization for collecting, managing, preserving, and sustaining access to digital content. This section identifies the benefit of the program to an institution and its relationship to other objectives, goals, and policies. *Links*: strategic plans, goals and objectives, budgets, preservation plans, technology plans.

Organizational Viability: addresses the legal status as well as human and other resources needed to establish and maintain a digital preservation program.

Scope: establishes the overall timeframe, levels of responsibility, boundaries, extent, limitations, and priorities of the digital preservation program. This section delineates what the organization's digital preservation program will do and, as importantly, will not do. The scope statement may be brief or extensive, depending on the nature of the program. The scope provides useful metric for measuring the effectiveness of the digital preservation program. *Links*: strategic plans, collection development policies, preservation plan, role definitions.

Operating Principles: defines the key principles, models, processes, and assumptions upon which the digital preservation program is developed and implemented. This section is particularly important in establishing system-wide benchmarks for distributed programs when multiple operational and technical processes are implemented. Common principles include adherence to standards (in particular OAIS) and other accepted indicators of good practice, support for life cycle management, interoperability, evidence-based requirements, and preferred methods of preservation. *Links*: community and organizational good practice, workflow and process documents, procedures.

Roles and Responsibilities: describes key stakeholders and their respective roles in digital preservation, including creators, producers, digital repository staff, administrators, financial managers, user groups, advisors, other repositories, and collaborators. This section makes an explicit statement that digital preservation is shared responsibility requiring participants within and beyond the organization. It describes broad categories of roles and responsibilities and cites documents containing more specific descriptions. *Links*: role definitions with explicit responsibilities, documentation of current role assignments, job descriptions, organizational charts.

Selection and Acquisition: provides the rationale and processes for developing and retaining collections based on specific parameters (e.g., formats, types of records, geographic scope). A clear articulation is critical to the success of a digital repository and ensures that collections support the institutional mission and priorities, and that requisite resources are made available for digital preservation. One aspect of auditing a digital archive is to verify that the stated mission and intended scope of a digital archive matches its actual content. Specific policies logically follow from the conceptual statement in the framework to further collection development aspects, e.g., submission guidelines. *Links*: collection development policy, submission guidelines, ingest workflow.

Access and Use: identifies the designated communities for the digital preservation program and the barriers and/or restrictions to use of the digital content for which the digital preservation program is responsible. Specific policies should be developed to further articulate access and use requirements and restrictions. *Note:* A digital archive may be dark, dim, or lit, but the absolute proof of preservation is in the capability to provide meaningful long-term access. *Links:* access policy, deposit agreements, digital rights management rules and practice, user agreements.

Challenges and Risks: identifies the organization's risks, difficulties, sense of urgency, and incentives for developing a digital preservation program. This section provides evidence that even though the full process may not be clearly understood, the need to act now is strong. *Links:* risk analyses, SWOT analyses, growth projections, examples of loss and near misses.

Financial Sustainability: documents the tangible basis for sustaining the digital preservation program.

Institutional Commitment: confirms and synthesizes the support for the program and the resources available to sustain the digital preservation program. *Links:* budgets, financial reports, fiscal policies, annual reports, succession plans, contracts

Cooperation and Collaboration: acknowledges that the organization's effort exceeds or will exceed available resources and may not guarantee the safety of all vital assets. This section places the digital preservation programs into a broader context that recognizes the program's dependencies on other partners and on the community at large. Collaborations and partnerships may require formal, legally binding agreements that delineate explicit roles and responsibilities of each party. *Links:* partnership agreements, operating principles and practices for collaborative projects.

Technological and Procedural Suitability: this component summarizes the preservation approach, strategies and techniques that are employed by the digital preservation program to achieve stated objectives. This section states the general philosophy of the digital preservation program and points to relevant requirements, policies, standards, guidelines, and practice. It makes a tangible link to the preservation planning component of the digital preservation program and to the organization's preservation plan. *Links:* preservation strategies, preservation plans for the organization and for specific content, deposit agreements.

System Security: specifies the organization's commitment and approach to ensuring the accuracy, completeness, authenticity, integrity, and long-term protection of the organization's digital assets. *Links:* security policies and procedures, disaster plan

Procedural Accountability: acknowledges the need for and stipulates the means for ensuring the transparency and accountability of the digital preservation program's policies and operations.

Audit and Transparency: explicitly commits the organization to periodic self-assessments and audits to evaluate, measure, and adjust the policies, procedures, preservation approaches, and practices of the digital preservation program. Transparency enables self-assessments and audits. Self-assessments and audits improve

internal operations, facilitate external reviews, and contribute to the development of effective partnerships and collaborations. **Links:** audit and self-assessment schedules and results, strategic plans, preservation plans.

Framework Administration: describes the organization's policies and practice pertaining to the development, approval, maintenance of the policy framework over time, e.g., frequency of updates and reviews, maintenance roles, expiration dates. The framework has little value if it has not received the appropriate approvals and has not been implemented. At minimum, the date and source of approval and the review cycle should be provided. **Links:** policy administration procedures, policy approval documentation.

Definitions: identifies terms and concepts that may be needed to understand the framework and may be instrumental in strategies for securing institutional commitment. This is an optional section, but one that can be very important. It is particularly important to include legally required and other mandated terminology and definitions. The section may either provide or point to requisite definitions. **Links:** definitions developed by the organization, glossaries adopted by the organization.

References: provides citations for or pointers to key resources that were informed the development and application of the framework. This section identifies more detailed documents, both internal and external, that provide a deeper expression of the mission, underlying principles, illustrative processes, and sustaining roles. It may contain citations for these documents or point to a current list of relevant community standards and guidance. **Links:** cited resources, community lists of standards and practice.

Provenance of the Outline

This outline reflects the findings of the Cornell Digital Preservation Management workshop curriculum development project (co-developers, Anne R. Kenney and Nancy Y. McGovern, with funding from the National Endowment for the Humanities); lessons learned in the development of the Cornell University Library Digital Preservation Policy Framework (<http://www.library.cornell.edu/iris/dpo/>); and samples of policy frameworks developed by organizations that participated in the Cornell DPM workshop, e.g., the Library and Archives of Canada, N.C. State Library.

References:

Open Archival Information System (OAIS) Reference Model, the January 2002 version is available at: http://nost.gsfc.nasa.gov/isoas/ref_model.html.

Attributes of a Trusted Digital Repository: Roles and Responsibilities, May 2002, available at: <http://www.rlg.org/longterm/repositories.pdf>.

Audit Checklist for Certifying Digital Repositories, January 2006 version available at: http://www.rlg.org/en/page.php?Page_ID=20769.