University of Maryland Libraries: Digital Preservation Policy

First rev. July 28, 2013
Approved by the Library Management Group: January 7, 2014
Second rev. July 28, 2014

Digital Preservation Policy Task Force:

Joanne Archer (2013, 2014)
Jennie Levine Knies (2013, 2014)
Carla Montori (2013)
Vin Novara (2013)
Robin Pike (2013, 2014)

Table of Contents

Mission

The University of Maryland (UMD) Libraries, in keeping with its mission "To enable the intellectual inquiry and learning required to meet the education, research and community outreach mission of the university," serves as a trusted caretaker of the UMD Libraries' collections, including those in digital format. The Digital Preservation Policy supports this mission and is the highest-level digital preservation policy document in the UMD Libraries. The Policy makes explicit the UMD Libraries' commitment to preserving content selected for retention by collection managers. It defines a comprehensive digital preservation program for both born-analog and born-digital collections. The audience for this policy includes UMD Libraries employees, digital content contributors, donors, and users.

Mandate

The American Library Association (ALA) defines Digital Preservation as the "policies, strategies, and actions to ensure access to reformatted and born-digital content regardless of the challenges of media failure and technological change. The goal of digital preservation is the accurate rendering of authenticated content over time."

The mandate for digital preservation at the UMD Libraries is linked to institutional responsibility, legal obligations, scholarly commitment, contractual obligations and grants, and membership services (…). The UMD Libraries' Strategic Plan (rev. 2013) contains a number of goals and objectives that imply the importance of digital preservation, including Goal I.4: "Exercise the Libraries' stewardship responsibilities, especially as they relate to developing and managing specialized collections," and Objective I.9.iv: Develop preservation plans for collections, including bit-preservation, digital object preservation, and metadata management pertaining to preservation of digital objects and their aggregation.

Digital Preservation Objectives

The UMD Libraries defines the primary objective of digital preservation activities as the ability to meaningfully access digital collection content over time. We will provide authenticity, discovery, and access to digital assets for current and future generations. This encompasses the following activities:

- Bit-level preservation of all digital objects, which means keeping the original files intact and which includes regular checks on the integrity of stored content;
- Ensuring that authenticity and provenance is maintained;
- Enabling uninterrupted (not necessarily instant) access to digital content over time as technology for digital content evolves.
- Complying with standards and best practices of the digital preservation community.
- Periodic review of preferred digital formats and digital metadata standards.
- Collaborating with campus, regional and national partners to make the best use of resources and avoid duplication of effort.

Financial Commitment

Enduring preservation of digital assets requires substantial and ongoing resource management over time. We are working towards metrics to allow more precise measurement of the real costs of providing a range of digital preservation services from bit-level preservation to full preservation, based on priorities, content, format, and other factors. Resources are needed throughout the lifecycle of digital assets to conduct periodic cost, risk, and value assessment of content selected by collection managers for digital preservation. This includes:

- Appraisal of digital assets to determine duration of digital preservation and access
- Supporting digital preservation by committing adequate financial and organizational resources
- Technical infrastructure
- Data preparation and validation
- Data management

Scope of Digital Preservation at the UMD Libraries

The UMD Libraries' Collection Development Policy states that "The University of Maryland Libraries is committed to ensuring the preservation and long-lasting availability of its research collections and resources in all formats." Preservation decisions are always made within the context of the Library's collection development policies, balancing costs and the limitations of resources, historical and scholarly value of the materials, and the needs of users.

The UMD Libraries' shall preserve digital assets:

- created using any type of application or on any computing platform
- delivered on any digital media;
- unique to the University of Maryland Libraries' collections;
- in danger of obsolescence or loss.

Challenges of Digital Preservation at the UMD Libraries

The preservation of digital assets represents a significant challenge. The inherent instability and vulnerability of digital assets affects the ways in which the UMD Libraries secures, manages, and preserves digital assets. In many cases, the UMD Libraries acquires digital content months, years, or even decades after the point of creation, which leads to scenarios affecting the level of risk, including:

- The carriers used to store digital assets are usually unstable and deteriorate within a few years or decades at most.

- The use of digital assets requires specific combinations of hardware and software that typically become obsolete after a few years, rendering the digital assets inaccessible.
- File formats change over time, which can mean that the digital assets are inaccessible using current software.
- File formats are sometimes unable to be determined, especially for older software.
- Digital assets may be lost in the event of disasters such as fire, flood, equipment failure, or virus or direct attack that disables stored data and operating systems.
- Access barriers such as password protection, encryption, and security devices may prevent ongoing access beyond the circumstances for which they were designed.
- The digital assets may be well protected, but so poorly identified and described that potential users cannot find them.
- So much contextual information may be lost that the assets themselves are unintelligible or not trusted.

The UMD Libraries will continually work to mitigate these risks through policy and technological development.

Roles and Responsibilities

The action and tasks of preserving digital content requires collaboration between staff throughout the UMD Libraries and with external organizations. Four high-level roles exist within our digital preservation ecosystem:

- *producers* are content owners or creators who submit content directly to the repository, for example, to the institutional repository (DRUM);
- *collection managers* are librarians who are responsible for appraising, selecting, and curating content;
- *administrative managers* are preservation, technical services, and information technology staff who design, enable, and carry out the workflows to ensure that preservation occurs;
- and *consumers* are the people who ultimately will use the content.

These four relationships are governed by policies approved and supported by the Library Managers Group (LMG). Specific responsibilities will be detailed in job descriptions, collection policies and through other official planning documents.

Training and Education

The UMD Libraries aims to support educational opportunities related to digital preservation that focus on five areas: general awareness; information lifecycle management; information storage management and systems; maintenance, best practices and standards; and legal issues and university policies.

Review and Evaluation

A group consisting of representatives from the primary stakeholder groups listed under "Roles and Responsibilities" will review policies and metrics annually.

Implementation Strategy

The UMD Libraries Digital Preservation Policy is the highest-level document defining the UMD Libraries' overarching philosophy regarding digital preservation. When we think about our "repository," we are referring to all of the different systems, both local and remote, used to manage our digital assets. Implementation of this policy will require a detailed digital preservation plan that incorporates a number of supplemental policy and procedure documents. It is recommended that the UMD Libraries follow the National Digital Stewardship Alliance's *Levels of Preservation* and the Trustworthy Repositories Audit and Certification (TRAC): Criteria and Checklist as a framework for outlining the types of policies and procedures that will together comprise a comprehensive digital preservation program at the UMD Libraries. A draft outline is located in Appendix A and Appendix B.

Resources/Acknowledgments

- Bishoff, Liz. "Digital Preservation Plan." Information Standards Quarterly 22, no. 2 (2010): 20-25.
- British Library *Digital Preservation Strategy* (http://www.bl.uk/aboutus/stratpolprog/collectioncare/digitalpreservation/strategy/dpstrategy.html). Last accessed, July 2014.
- Center for Research Libraries, *Metrics for Repository Assessment* (http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac). Last accessed, July 2014.
- Consultative Committee for Space Data Systems. (2012). Reference Model for an Open Archival Information System (OAIS). Washington, DC: CCSDS Secretariat (http://public.ccsds.org/publications/archive/650x0m2.pdf). Last accessed, July 2014.
- Hathi Trust *Digital Preservation Policy* (http://www.hathitrust.org/preservation). Last accessed, July 2014.
- McGovern, Nancy Y. *Version 2.0 Digital Preservation Policy Framework: Outline*, ICPSR, January 2007 (last revised October 2007) (http://www.icpsr.umich.edu/files/ICPSR/curation/preservation/policies/dp-policy-outline.pdf). Last accessed, July 2014.
- National Archives of Australia, *Digital Preservation Policy*, 4th Edition, 2013 (http://www.nla.gov.au/policy-and-planning/digital-preservation-policy). Last accessed, July 2014.
- Owens, Trevor. *NDSA Levels of Digitization, Release Candidate One*, November 20, 2012 (http://blogs.loc.gov/digitalpreservation/2012/11/ndsa-levels-of-digital-preservation-release-candidate-one/). Last accessed, July 2014.
- Shepherd, Kelcy. "Preserving Digital Archives," Digital Archives Specialist course packet, Society of American Archivists, 2014
- University of Utah, *Digital Preservation Policy* (http://www.lib.utah.edu/collections/digital/digital-preservation.php). Last accessed, July 2014.
- Yale University Library, *Policy for Digital Preservation*, 2007. (http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf). Last accessed, July 2014.

Appendix A. National Digital Stewardship Alliance, Version 1 of the Levels of Preservation.

This document, created by the National Digital Stewardship Alliance (http://digitalpreservation.gov/ndsa/activities/levels.html), is a "tiered set of recommendations for how organizations should begin to build or enhance their digital preservation activities." The UMD Libraries will use this document as a method of assessing our current digital preservation activities, and as a way to justify and document additional practices moving forward. These may be used in conjunction with AVPreserve's document that maps the NSDA levels of digital preservation and the ISO 16363:2012 requirements.

Table 1: Version 1 of the Levels of Digital Preservation

	Level 1 (Protect your data)	Level 2 (Know your data)	Level 3 (Monitor your data)	Level 4 (Repair your data)
Storage and Geographic Location	- Two complete copies that are not collocated - For data on heterogeneous media (optical discs, hard drives, etc.) get the content off the medium and into your storage system	- At least three complete copies - At least one copy in a different geographic location - Document your storage system(s) and storage media and what you need to use them	- At least one copy in a geographic location with a different disaster threat - Obsolescence monitoring process for your storage system(s) and media	- At least three copies in geographic locations with different disaster threats - Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems
File Fixity and Data Integrity	- Check file fixity on ingest if it has been provided with the content - Create fixity info if it wasn't provided with the content	- Check fixity on all ingests - Use write-blockers when working with original media - Virus-check high risk content	- Check fixity of content at fixed intervals - Maintain logs of fixity info; supply audit on demand - Ability to detect corrupt data - Virus-check all content	- Check fixity of all content in response to specific events or activities - Ability to replace/repair corrupted data - Ensure no one person has write access to all copies
Information Security	- Identify who has read, write, move and delete authorization to individual files - Restrict who has those authorizations to individual files	- Document access restrictions for content	- Maintain logs of who performed what actions on files, including deletions and preservation actions	- Perform audit of logs
Metadata	- Inventory of content and its storage location - Ensure backup and non-collocation of inventory	- Store administrative metadata - Store transformative metadata and log events	- Store standard technical and descriptive metadata	- Store standard preservation metadata
File Formats	- When you can give input into the creation of digital files encourage use of a limited set of known open formats and codecs	- Inventory of file formats in use	- Monitor file format obsolescence issues	- Perform format migrations, emulation and similar activities as needed

Appendix B. Adaptation of Metrics for Repository Assessment

The 2013 version of this policy contained an appendix that outlined the policies and procedures necessary to ensure that a digital preservation program runs successfully. See: Center for Research Libraries, *Metrics for Repository Assessment* (http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac). While we continue to use this as a guideline, we have decided to begin our work with the more straightforward NDSA Levels of Preservation in Appendix A.

A. Organizational Infrastructure

"Regardless of the size, scope, or nature of the digital preservation program, a trusted repository must demonstrate an explicit, tangible, and long-term commitment to compliance with prevailing standards, policies, and practices."

A1. Governance and Organizational Viability

Policy/Procedure	Responsibility	Notes
UMD Libraries Mission Statement	Dean's Office	
Explicit and specific statement documenting the intent to ensure continuity of the repository, and the steps taken and to be taken to ensure continuity	Digital Systems and Stewardship	
Formal documents describing exit strategies, contingency plans, and succession plans	Digital Systems and Stewardship	
Depositor agreements	Producers, Collection Managers	

A2. Organizational structure & staffing

Policy/Procedure	Responsibility	Notes
Roles and Responsibilities for Digital Preservation	Collection Managers, Administrative Managers	Outlined generally Digital Preservation Policy. A separate document should be more specific about who conducts which duties according to the UMD Libraries' organizational structure
Work plans, Planning Documents (Divisional, Departmental, Unit, and	All	

Individual)		
Job Descriptions (individual)	All	
Training resources	All	Professional Development
UMD Libraries' Organizational Charts	Dean's Office	
Digital Preservation Networks Policy	Administrative Managers/Digital Programs and Initiatives	Policy indicating where and how to account for digital assets (DPN, APT, HathiTrust, etc.)

A3. Procedural accountability & policy framework

Policy/Procedure	**Responsibility**	**Notes**
Designated Community, definitions (producer and user communities)	Collection Managers/Administrative Managers	
Digital Repository Policies	Administrative Managers (Digital Programs and Initiatives, Software Systems Development and Research	Includes: Documentation detailing review, update, and development mechanisms. Documentation in the form of policies, procedures, protocols, rules, manuals, handbooks and workflows. Change Management.
Deposit Agreements	Producers, Collection Managers	
Records Retention Schedules	Collection Managers	
Procedures for Integrity Measurements	Administrative Managers	
Service Level Policy	Administrative Managers	Tiers of service for digital preservation, format registry, migration policies
Intellectual Property	Collection Managers, Administrative Managers	A definition of rights; citations for relevant laws and requirements; policy on

		responding to challenges; documented track record for responding to challenges in ways that do not inhibit preservation; examples of legal advice sought and received

A4. Financial Sustainability

Policy/Procedure	Responsibility	Notes
Evidence of Commitment of Operations Budget for Digital Preservation	Library Resources Group	Financial reports, budgets, etc.
Risk Assessment Decision Matrix	Administrative Managers	
Risk Management Documents	Administrative Managers	Identify perceived and potential threats and planned or implemented responses
Technology infrastructure investment planning documents	Library Resources Group	
Cost/Benefit Analysis	Administrative Managers	
Requirements for and examples of Licenses, Contracts, and Asset Management	Collection Managers, Administrative Managers	
Commitment to membership in Digital Preservation Networks	Dean's Office	DPN, APTrust, HathiTrust, etc.

A5. Contracts, licenses, & liabilities

Policy/Procedure	Responsibility	Notes
Deposit Agreements	Producers, Collection Managers	Examples Include: • DRUM • Web Archiving • Born-Digital • Deed-of-Gift Agreements/Memoranda of Understandin • Research Data

Service Level Policy	Administrative Managers	Tiers of service for digital preservation, format registry, migration policies
Intellectual Property	Collection Managers, Administrative Managers	A definition of rights; citations for relevant laws and requirements; policy on responding to challenges; documented track record for responding to challenges in ways that do not inhibit preservation; examples of legal advice sought and received. Includes policies and procedures for dealing with challenges to rights
Policy on Exclusions from Digital Preservation Responsibility	Collection Managers/Administrative Managers	Partially covered by Digital Preservation Policy, for example, commercially-licensed content

B. Digital Object Management

"The digital object management responsibilities of a repository include both some 'organizational' and technical aspects related to these responsibilities, such as repository functions, processes, and procedures needed to ingest, manage, and provide access to digital objects for the long term."

- Documentation of standard operating procedures

B.1 Ingest: Acquisition of Content

Policy/Procedure	Responsibility	Notes
Ingest policies and procedures	Administrative Managers	Automated or manual workflow to ingest appropriate digital objects
Collection Policies/Retention Policies	Collection Managers	
Best Practices for Digital Collections at the University of Maryland Libraries	Administrative Managers (Digital Conversion and Media Reformatting)	

B.2 Ingest: Creation of the Archivable Package

Policy/Procedure	Responsibility	Notes
Digital Format Registry	Administrative Managers	
Documentation for identifying and preserving each class of archival information package (AIP)	Administrative Managers	

B.3 Preservation Planning

Policy/Procedure	Responsibility	Notes
Digital Preservation Policy/Plan		

B.4 Archival Storage and Preservation/Maintenance of AIPs

Policy/Procedure	Responsibility	Notes
Documentation for identifying and preserving each class of archival information package (AIP)	Administrative Managers	
Storage and Migration Strategies	Administrative Managers	Ensure effective capture, ongoing and reliable archival storage, and responsiveness to technological change

B.5 Information Management

Policy/Procedure	Responsibility	Notes
Metadata Policies, procedures and workflows	Collection Managers, Administrative Managers	Includes preservation, technical, administrative, and descriptive metadata
Processing procedures	Collection Managers/Administrative Managers	

B.6 Access Management

Policy/Procedure	Responsibility	Notes
Access and Use Policies	Collection Managers	
Policy on Recording Access Actions	Administrative Managers/Collection Managers	Workflow and tools for recording access actions

C. Technologies, Technical Infrastructure, & Security

"These requirements do not prescribe specific hardware and software to ensure AIPs can be preserved for the long term, but describe best practices for data management and security."

C1. System Infrastructures

C1.1 Repository functions on well-supported operating systems and other core infrastructural software.

Policy/Procedure	Responsibility	Notes
Software Inventory	Administrative Managers	
Support Contracts	Administrative Managers	
System Documentation	Administrative Managers	
Use of Strongly Community-Supported Software	Administrative Managers	

C1.2 Repository ensures that it has adequate hardware and software support for backup functionality sufficient for the repository's services and for the data held, e.g., metadata associated with access controls, repository main content.

Policy/Procedure	Responsibility	Notes
Documentation of what is being backed up and how often	Administrative Managers	Includes audit log/inventory of backups, validation, and testing
Disaster Recovery Plan	Administrative Managers	

C1.3 Repository manages the number and location of copies of all digital objects.

Policy/Procedure	Responsibility	Notes
Location register/log of digital objects compared to the expected number and location of copies of particular objects	Administrative Managers	
Random Retrieval Tests	Administrative Managers	

C1.4 Repository has mechanisms in place to ensure any/multiple copies of digital objects are synchronized.

Policy/Procedure	Responsibility	Notes
System analysis of how long it takes for copies to synchronize	Administrative Managers	
Procedures/documentation related to whether changes lead to the creation of new copies and how those copies are propagated and/or linked to previous versions	Administrative Managers	

C1.5 Repository has effective mechanisms to detect bit corruption or loss.

Policy/Procedure	Responsibility	Notes
Documents that specify bit error detection and correction mechanisms used	Administrative Managers	

C1.6 Repository reports to its administration all incidents of data corruption or loss, and steps taken to repair/replace corrupt or lost data.

Policy/Procedure	Responsibility	Notes
Preservation Metadata Records	Administrative Managers	

C1.7 Repository has defined processes for storage media and/or hardware change (e.g., refreshing, migration).

Policy/Procedure	Responsibility	Notes
Documentation of processes; policies related to hardware support, maintenance, and replacement	Administrative Managers	

C1.8 Repository has a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.

Policy/Procedure	Responsibility	Notes
Change Management Process Documentation	Administrative Managers	Handled in JIRA via LCAB (Libraries Change Advisory Board)

C1.9 Repository has a process for testing the effect of critical changes to the system.

Policy/Procedure	Responsibility	Notes
Documented Testing Procedures	Administrative Managers	Handled in JIRA via LCAB (Libraries Change Advisory Board)

C1.10 Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment.

Policy/Procedure	Responsibility	Notes
Risk Register	Administrative Managers	List of all patches available and risk documentation analysis
Evidence of Update Processes	Administrative Managers	For example: server update manager daemon
Documentation related to the Update Installations	Administrative Managers	

C2. Appropriate Technologies

Policy/Procedure	Responsibility	Notes
Technology watch	Administrative Managers	
Documentation of procedures	Administrative Managers	
Designated community profiles	Collection Managers, Administrative Managers	
User needs evaluation	Collection Managers, Administrative Managers	
Hardware inventory	Administrative Managers	
Process to monitor required hardware and software changes	Administrative Managers	

C3. Security

Policy/Procedure	Responsibility	Notes
Disaster and Recovery Planning	Administrative Managers	
Service Continuity Plan	Administrative Managers	
Documentation Linking Roles with Activities	Administrative Managers	
Local geological, geographical, or meteorological data or threat assessments	Administrative Managers	
Proof of at least one off-site copy of preserved information	Administrative Managers	If level of preservation calls for this