

Best Practices for Digital Collections Resources

October 5, 2018

Corinne Jacox,
Catalog/Reference Librarian,
Creighton University Law Library
corinnejacox@creighton.edu

Yumi Ohira,
Digital Initiatives Librarian
University of Nebraska at Omaha Libraries
yohira@unomaha.edu

Metadata Best Practices

Best Practices for CONTENTdm and Other OAI-PMH Compliant Repositories: Creating Sharable Metadata Version 3.1 (OCLC 2013)

<https://www.oclc.org/support/training/portfolios/digital-collection-management/contentdm.en.html>

CDP Metadata Working Group Dublin Core Metadata Best Practices Version 2.1.1 (2006)

<https://www.lyrasis.org/services/Pages/Digital-Toolbox-Metadata.aspx>

Lyrassis Digital Toolbox Metadata

<https://www.lyrasis.org/services/Pages/Digital-Toolbox-Metadata.aspx>

Mountain West Digital Library Dublin Core Application Profile Version 2.0 (2011)

<https://mwdl.org/getinvolved/guidelines.php>

Nebraska Library Commission Nebraska Memories Metadata Guidelines (2009)

<http://nlc.nebraska.gov/nebraskamemories/metadata.aspx>

Nebraska Library Commission Digitization Resources

<http://www.nlc.state.ne.us/libman/digitization.aspx>

Orbis Cascade Alliance Dublin Core Best Practice Guidelines Version 2.3 (2018)

<https://www.orbiscascade.org/dublin-core-best-practices/>

Policies

University of Hawai'i at Mānoa Library

<https://guides.library.manoa.hawaii.edu/c.php?g=105219&p=687076>

University of Chicago Library

<https://www.lib.uchicago.edu/research/scholar/digitalscholarship/institutional-repository/institutional-repository-policies/>

NDSA Report “The Benefits and Risks of the PDF/A-3 File Format for Archival Institutions”

<https://blogs.loc.gov/thesignal/2014/02/new-nds-report-the-benefits-and-risks-of-the-pdf-a-3-file-format-for-archival-institutions/>

Level of Digital Preservation: <https://ndsa.org/activities/levels-of-digital-preservation/>

<https://ndsa.org/activities/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	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - At least one copy in a geographic location with a different disaster threat - Obsolescence monitoring process for your storage system(s) and media 	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Check file fixity on ingest if it has been provided with the content - Create fixity info if it wasn't provided with the content 	<ul style="list-style-type: none"> - Check fixity on all ingests - Use write-blockers when working with original media - Virus-check high risk content 	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Identify who has read, write, move and delete authorization to individual files - Restrict who has those authorizations to individual files 	<ul style="list-style-type: none"> - Document access restrictions for content 	<ul style="list-style-type: none"> - Maintain logs of who performed what actions on files, including deletions and preservation actions 	<ul style="list-style-type: none"> - Perform audit of logs
Metadata	<ul style="list-style-type: none"> - Inventory of content and its storage location - Ensure backup and non-collocation of inventory 	<ul style="list-style-type: none"> - Store administrative metadata - Store transformative metadata and log events 	<ul style="list-style-type: none"> - Store standard technical and descriptive metadata 	<ul style="list-style-type: none"> - Store standard preservation metadata
File Formats	<ul style="list-style-type: none"> - When you can give input into the creation of digital files encourage use of a limited set of known open formats and codecs 	<ul style="list-style-type: none"> - Inventory of file formats in use 	<ul style="list-style-type: none"> - Monitor file format obsolescence issues 	<ul style="list-style-type: none"> - Perform format migrations, emulation and similar activities as needed