The Levels of Digital Preservation

The "**Levels of Digital Preservation**" are a tiered set of recommendations for how organizations should begin to build or enhance their digital preservation activities. A work in progress by the NDSA, it is intended to be a relatively easy-to-use set of guidelines useful not only for those just beginning to think about preserving their digital assets, but also for institutions planning the next steps in enhancing their existing digital preservation systems and workflows. It allows institutions to assess the level of preservation achieved for specific materials in their custody, or their entire preservation infrastructure. It is not designed to assess the robustness of digital preservation programs as a whole since it does not cover such things as policies, staffing, or organizational support. The guidelines are organized into five functional areas that are at the heart of digital preservation systems: storage and geographic location, file fixity and data integrity, information security, metadata, and file formats.

See the **Levels, Table Version 1** on the reserve side.

Resources:

The NDSA Levels of Digital Preservation: An Explanation and Uses
http://www.digitalpreservation.gov/ndsa/working_groups/documents/NDSA_Levels_Archiving_2013.pdf

Blog Series on *The Signal* on how to go about working your way through the cells on each level

- Protect Your Data: Storage and Geographic Location, Dec. 24, 2013: http://blogs.loc.gov/digitalpreservation/2013/12/protect-your-data-storage-and-geographic-location/
- Protect Your Data: File Fixity and Data Integrity, Apr. 7, 2014: http://blogs.loc.gov/digitalpreservation/2014/04/protect-your-data-file-fixity-and-data-integrity/
- Protect Your Data: Information Security and the Boundaries of your Storage System, Apr. 16. 2014: http://blogs.loc.gov/digitalpreservation/2014/04/protect-your-data-information-security-and-the-boundaries-of-your-storage-system/

Organizations Using the Levels

- The Levels of Digital Preservation and the Truth and Reconciliation Commission of Canada, Aug. 21, 2013: http://blogs.loc.gov/digitalpreservation/2013/08/the-levels-of-digital-preservation-and-the-truth-and-reconciliation-commission-of-canada/
- NDSA Levels of Digital Preservation @ USGS: An interview with John Faundeen, July 11, 2013: http://blogs.loc.gov/digitalpreservation/2013/07/ndsa-levels-of-digital-preservation-usgs-an-interview-with-john-faundeen/

How the Levels Developed

- Help Define Levels for Digital Preservation, Sept. 7, 2012: http://blogs.loc.gov/digitalpreservation/2012/09/help-define-levels-for-digital-preservation-request-for-public-comments/
- NDSA Levels of Digital Preservation Release One Candidate, Nov. 20, 2012: http://blogs.loc.gov/digitalpreservation/2012/11/ndsa-levels-of-digital-preservation-release-candidate-one/
- What Would You Call the Last Row of the NDSA Levels of Digital Preservation, July 15, 2013: http://blogs.loc.gov/digitalpreservation/2013/07/what-would-you-call-the-last-row-of-the-ndsa-levels-of-digital-preservation/

NDSA

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 you 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 it is 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	-Storage standard technical and descriptive metadata	-Store standard preservation metadata
File Formats	-What 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

http://www.digitalpreservation.gov/ndsa/activities/levels.html

NDSA