The University of British Columbia Library		Document No.	DP-006
		Approval Date	*May 5, 2016*
		Last Revision	*May 25, 2017*
Title	Levels of Digital Preservation		

OBJECTIVES

- ❑ Aid in organizing and mitigating digital preservation risks
- ❑ Levels can be applied to specific collections and/or system wide
- ❑ Levels are content and system agnostic

LEVEL 1

Resources preserved at this level are subject only to bit-level preservation activities. Under this level, a resource will be subject to virus checks and regular backups. Only select metadata is archived along with the resource. This is a basic level of preservation which ensures stores copies of resources and regular backups of the resources. Multiple copies of a resource are retained to encounter the perils of media decay. This level of preservation lacks advanced preservation activities like format normalization, format migration, validation checks and full metadata.

LEVEL 2

Level 2 preservation is intended for resources that require medium to long-term preservation but are currently being preserved elsewhere and/or have lower projected preservability. Resources within this plan undergo virus checks, integrity checks, file normalization, and include extended metadata. Active monitoring is not part of this plan, and it also lacks any normalization or migration strategies. Multiple copies help to encounter the problem of media decay and ensure bit-level preservation.

LEVEL 3

Resources preserved at this level are subject to a rich set of preservation actions for long-term accessibility. Upon ingest, a resource

will go through virus checking, fixity checking, file validation, format normalization and archival packaging processes. Level 3 resources are archived with full metadata to capture information about the resource, provenance, authenticity, preservation activity, technical environment and rights. To prevent a loss of access to files due to file format obsolescence, all resources at Level 3 are subject to a file format migration strategy, which helps to keep the content stored in formats that are readable by the current technology.

	Level 1: Basic Preservation	**Level 2: Bit-level Plus Preservation[1]**	**Level 3: Full Preservation**
Type of content	❑ external digitization requests ❑ legacy digitized content ❑ selected/licensed research data sets ❑ in copyright material ❑ file format conversion projects ❑ licenced data sets	❑ other locally digitized resources (e.g., retrospectively scanned newspapers) ❑ low quality files ❑ material of lower projected preservability	❑ flagship digitization projects representing collections of local strength ❑ locally created born digital collections ❑ externally created resources for which we have stewardship responsibilities i.e. Chinese Canadian Stories Community Collections ❑ COPPUL PLN content (200 GB) ❑ CGI PLN content (consortial) ❑ select research data sets (DataVerse)
Storage and Geographic Location	❑ 2 complete copies ❑ transfer from heterogeneous media to storage system	❑ 3 complete copies ❑ 1 copy in different geographic location ❑ document storage system	❑ crash consistent snapshot is taken every morning at 3am and vaulted over to a remote location at midnight the same day

[1] UBC Library currently implements Level 1 and Level 3 Preservation, but intends on employing Level 2 as appropriate when the need arises.

	❑ Document your storage system(s) and storage media and what you need to use them	❑ Start an obsolescence monitoring process for your storage system(s) and media	❑ Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems.
File Fixity and Data Integrity	❑ Virtual Server storage (Backup snapshots to disk are performed daily and weekly. Daily backups are stored for 28 days while weekly snapshots are kept for 12 weeks.) ❑ No Fixity Checking, No Data Integrity	❑ Check 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 at fixed intervals ❑ use write-blockers when working with originals ❑ maintain logs of fixity info; supply audit on demand ❑ ability to detect corrupt data ❑ virus check all content (Bag-it or some other tool)	❑ Snapshots allow you to preserve the state of the virtual machine so you can return to the same state repeatedly. ❑ Please note that snapshots are not backup systems – they only contain deltas of changes between the time the snapshot was taken and current state. ❑ Archivematica micro-services/tools: fixity checks, specifically Transfer micro-service "Assign file UUIDs and checksums" (which assigns a sha-256 checksum to each transfer) and Ingest micro-service "Verify checksums." Archivematica micro-services use md5deep to generate and verify

			checksums ❑ Materials stored in Archivematica are subject to regular fixity checks – comparisons of checksum values calculated at a given point in time with those generated at time of ingest. To check fixity of AIPs in storage, Artefactual has a separate command-line app called Fixity (further user documentation for Fixity is pending).
Information Security	❑ identify who has read, write, move and delete authorization to individual files ❑ restrict who has authorizations to individual files	❑ document access restrictions for content ❑ maintain logs of who accessed, edited files, including deletions and preservation actions	❑ 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 ❑ create minimal metadata for access	❑ store administrative metadata ❑ Store transformative metadata and log events ❑ store standard technical and descriptive metadata	❑ store standard preservation metadata

File Formats	❑ encourage use of archival and open formats and codecs	❑ inventory of file formats in use ❑ Validate files against their file formats ❑ monitor file format obsolescence issues on an on-going basis	❑ perform format migrations, emulation and similar activities as needed

Sources Consulted

Library of Congress' Levels of Digital Preservation: A tool for mitigating technical digital preservation tools
https://blogs.loc.gov/digitalpreservation/files/2012/09/Levels-of-Digital-Preservation-draft-handout-v3.pdf

University of Alberta's Tiered Preservation Model
http://purl.pt/24107/1/iPres2013_PDF/TAP%20A%20Tiered%20Preservation%20Model%20for%20Digital%20Resources.pdf