

NDSA Levels of Digital Preservation Mapped to Tools and Policy Recommendations

Levels created by the [National Digital Stewardship Alliance](#)

Tools and Policy Recommendations created by Alice Prael, Shira Peltzman and the Digital Preservation Community --*please make your own recommendations!*

	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
	<ul style="list-style-type: none"> - Strategic Plan and schedule for ingesting content into storage system 	<ul style="list-style-type: none"> -Storage Tools from COPTR -Inventory of physical media and digital files 	<ul style="list-style-type: none"> -Storage Tools from COPTR -Digital Preservation Policy should include a timeline for monitoring storage obsolescence 	<ul style="list-style-type: none"> -Storage Tools from COPTR - Exit Strategy/Digital Disaster Recovery Plan
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
	<ul style="list-style-type: none"> -AV Preserve's Fixity -File Analyzer and Metadata Harvester - Library of Congress's Bagger 	<ul style="list-style-type: none"> -AV Preserve's Fixity -Clam AV for virus scanning 	<ul style="list-style-type: none"> -AV Preserve's Fixity -Clam AV for virus scanning 	<ul style="list-style-type: none"> -AV Preserve's Fixity -Policy for replacing corrupted data from preservation storage -Access Policy to manage write access to digital holdings
Information Security	<ul style="list-style-type: none"> - Identify who has read, write, move 	<ul style="list-style-type: none"> - Document access restrictions for 	<ul style="list-style-type: none"> - Maintain logs of who performed 	<ul style="list-style-type: none"> - Perform audit of logs

	and delete authorization to individual files - Restrict who has those authorizations to individual files	content	what actions on files, including deletions and preservation actions	
	- Access Policy - Preservation System or DAMS should manage authorizations at the file level	- Access Policy	Preservation System or DAMS should create and maintain action logs	Digital Preservation Policy should mandate auditing of action logs at fixed intervals
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
	Digital Preservation Outreach & Education inventory example Digital Preservation Management Workshop inventory example	Metadata policy and data dictionaries	Metadata policy and data dictionaries FITS - File Information Tool Set extracts embedded technical metadata	PREMIS
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
	PRONOM Library of Congress - Sustainability of Digital Formats	FITS - File Information Tool Set Digital Preservation Policy should outline acceptable digital formats	NARA Guidance for Digital File Formats PRONOM Library of Congress - Sustainability of Digital Formats	NDSA Migration Checklist Signal Blog on Format Migrations at Harvard