Levels of Digital Preservation Preparedness

This resource is a guide to understanding digital preservation, with a focus on three different levels of preparedness. This resource will help you to start minimal digital preservation steps at your institution, and show how to build upon digital preservation incrementally.

For more information about digital preservation procedures, tools, and policies, view related items connected to this resource on the Sustainable Heritage Network in the "Digital Preservation" category.

- The Three Essentials of Digital Preservation
- Activities to Include in a Digital Preservation Plan
- Digital Preservation Glossary
- Developing a Digital Preservation Policy

Introduction

Digital preservation is a series of activities, plans, and policies combined to ensure continued preservation and access of digital materials. Organization and management of digital files is just as important as any other format type. In fact, digital files can be even more vulnerable than a piece of paper or photograph.

This document suggests the following levels of preparedness:

- **Level 1: Minimum Digital Preservation** provides basic recommendations for making a plan for digital preservation with minimal amounts of time, resources and support.
- **Level 2: Intermediate Digital Preservation** provides additional recommendations including making a plan for digital preservation with more time, resources, and support. At this level there may be some funding to purchase equipment or tools, time to plan, and interest from others in your department, institution, or community to define your preservation goals and needs.
- **Level 3: Advanced Digital Preservation** provides recommendations that will complete your digital preservation plan and provide dependable and long-term protection for digital content. At this level you have the time, resources, and

support you need to meet all digital preservation needs, and are able to consult with others outside your institution.

Within each level of preparedness, there are sections of **File Storage**, **File Integrity**, and **File Access**. Each section has several digital preservation activities or features listed for the appropriate level. The sections include:

- **File Storage:** *Making sure that digital content chosen for long term preservation is stored safely and securely.*
  - File storage addresses physical storage systems, location of storage, and use of multiple physical storage locations to prevent or minimize data loss due to storage device failure or natural disaster.
- **File Integrity:** *Ensuring the stability of digital content over time.*
  - File integrity addresses stability of data, concerns about data corruption and alteration, as well as prevention, detection, and recovery of changed data.
- **File Access:** *Organizing and describing digital files so that current and future staff will be able to find, access, understand, and use digital content.*
  - File access addresses security of data, documentation of data, file formats, data structures and naming conventions.

Each of these sections of digital preservation can each be targeted for a different level of preparedness at your institution. Different parts of digital collections can also be at different levels. For example, different projects or departments may have different backup schedules or requirements; some projects might require much tighter security restrictions than others; and in some cases, the best recommendation might be beyond your current financial or technical scope, or simply may not be relevant to your situation.

While reading through the three levels of preparedness (minimum, intermediate, and advanced), keep in mind that the the intermediate and advanced levels add on to the basic recommendations in the minimum level of digital preservation. A complete digital preservation plan would include information building from all levels.

Minimum Digital Preservation

Minimum Digital Preservation focuses on having basic steps in place, and knowing foundational information about your digital files. If your institution is just beginning with digital preservation planning, only have a limited amount of digital content, or simply do not have the time or resources to dedicate to digital preservation, this level of digital preservation is well suited for your institution.

File Storage

- Store two complete copies of digital files in different geographic locations.
- Transfer data off of different types of media as it comes into your institution (CDs/DVDs, hard drives, floppy discs, etc.) and save on your storage system.
- Understand what storage systems are available to store digital content.
    - Talk with IT, administration, or other departments to discuss what digital storage is currently in place and who is involved in managing and supporting digital storage.
- Inventory all media currently used to store digital files, including hard disks.
    - Take an inventory of every location that digital files are stored, size of files, and what types of storage media (hard drives, flash drives, internal hard drives on a computer, server storage, etc.)
    - An inventory of storage media will help you identify priorities for transferring off unstable media like CDs and DVDs, floppy discs, flash drives.
    - This inventory can be on a spreadsheet or any other system used at your institution for organization of files and material.
- Create a basic emergency or disaster plan that considers what will happen if a storage device fails.

File Integrity

- Check fixity of file on ingest if it has been provided with the content.
- Create fixity information if it has not been provided with the content. For example, use a tool like Fixity or MD5Summer to create a checksum for a file or files. Then, store that information in the same location as the file or in a spreadsheet.

File Access

- Identify who has read, write, move, and delete authorization to individual files. This should be by roles, for example: the head archivist and the media specialist.
- Restrict authorizations to only necessary people.
- Create and update an inventory of content and its storage location (make sure this inventory is backed up along with digital files).
- Create an inventory of file formats in use.
- Encourage use of a limited set of known and open file formats.
    - An open format is a file format that can be used and implemented by anyone. Proprietary formats, on the other hand, are designed to be

    controlled by a particular company, might only be able to be opened using that company's software, are not a good choice for long term preservation.
    - For example: Your file format policy might include always using a TIFF or JPEG2000 file format for image files, instead of a PSD file (Adobe Photoshop's proprietary file format for project files). This is because TIFF and JPEG2000 are formats that are widely used and will be supported into the future.

Intermediate Digital Preservation

The **Intermediate Digital Preservation** level builds onto the basics with more detailed planning, storage, organization, and security for digital files. If you are ready to add more robust steps to digital preservation plans, and have an increased amount of time or resources to dedicate to digital preservation, this level of digital preservation might work well for your institution.

File Storage

- Follow the **3-2-1 Rule** for digital storage:
    - Keep **three** copies of any content that will be preserved for the long term.
    - Stored on **two** types of storage media.
    - With **one** of the three copies stored in a different geographic location.
- Research and evaluate storage media suitable for your preservation needs, purchase storage media as needed.
- Start a process or schedule to monitor all storage systems and media, and migrate storage when needed.
    - All storage media has a risk of failure, and a recommended life span. For example: most single hard drives will fail after 3-5 years.
    - Find out what the manufacturer's recommendation is for all storage media and systems, and create a plan to replace and transfer digital content.
- Transition away from media that are 10 or more years old.
- Create a emergency or disaster plan that covers each section of digital preservation planning.
    - For more information on emergency and disaster planning, view the following resources on the SHN website:
        - Writing Your Disaster Plan
        - Wind: Preparation and Partnerships in Emergency Planning
        - Museum Core Documents: Emergency Plan

File Integrity

- Check fixity on all ingests of digital files.
- Use writeblockers when working with original media.
    - A write blocker allows for a transfer of files from another storage media onto a computer without being able to write to the original storage media. There are both hardware and software write blockers.
- Perform virus checks on high risk content.

File Access

- Maintain logs of who has accessed individual files.
- Store metadata about digital content. Metadata can be recorded in spreadsheets, databases, or embedded in files.
    - Store administrative, technical, and descriptive metadata for digital content.
- Validate files against their file formats with software validation tools.
- Monitor file format obsolescence threats, keep up to date with the latest file formats.

Advanced Digital Preservation

The **Advanced Digital Preservation** level provides a comprehensive list of digital preservation activities and planning goals. If you have most of the steps in the Intermediate level in place, and have funding, support, and time to commit, then this level will be helpful in making your digital preservation plan as complete as possible.

File Storage

- At least one copy (ideally all) in a geographic location with a different disaster threat.
- Create and update a comprehensive plan that will keep files and metadata on currently accessible media or systems.
- Transfer files off of all obsolete storage media devices, and properly dispose.
- Ensure that all information is migrated from an older media to a newer media, on a set schedule, including hard disks (follow manufacturer's recommendations).
- Create and follow a detailed emergency or disaster plan and run tests or simulations to be prepared.

File Integrity

- Check fixity after any transformative acts.
- Check fixity of sample files/media at fixed intervals.

- Maintain logs of fixity information and supply audit on demand.
- Virus check all content.
- In emergency situations:
  - Check fixity of all content in response to specific events or activities.
  - Have a plan in place to replace corrupted data.

File Access

- Maintain logs of who performed what actions on files, including deletions and preservation actions.
- Perform audit of logs.
- Store standard preservation metadata along with descriptive and other metadata using your institution's chosen method (which might be spreadsheets, database, CMS, etc.)
- Perform file format migrations if file formats become outdated or unsupported.
- Perform emulation, if file migration does not produce the intended results. Emulation involves using a program that imitates the original, obsolete hardware or software to open and view a digital file.

Conclusion

In an ideal world, every institution could plan for the highest level of digital preservation for all content. However, with vast amounts of digital files to manage, and many other responsibilities, this is not realistic for every institution. Digital preservation depends on many factors within your institution including staff time, funding, technology, support, and balancing other priorities. Every step in the **Advanced** or **Intermediate Digital Preservation** levels may not be attainable right away, but there may be certain activities from all sections in this document that you are able to include in plans to strengthen digital preservation at your institution.

Other Useful Resources

The NDSA Levels of Digital Preservation: An Explanation and Uses, by Megan Phillips, Jefferson Bailey, Andrea Goethals, and Trevor Owens, *Archiving Conference*. Vol. 2013. No. 1. Society for Imaging Science and Technology, 2013.
A tiered set of recommendations on how organizations should begin to build or enhance their digital preservation activities.