Activities to Include in a Digital Preservation Plan

Digital preservation includes a series of policies, strategies, and activities that combine to ensure that your digital collections remain usable, authentic, discoverable, and accessible over time. This document contains a list of activities involved in the many stages of digital preservation. These activities help define what actions can be taken at your institution to preserve digital files including first steps like discussing preservation needs, inventorying digital content, and purchasing storage media. These activities help create a long term digital preservation plan for your cultural institution that reflects your priorities and goals.

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
- Levels of Digital Preservation Preparedness
- Digital Preservation Glossary
- Developing a Digital Preservation Policy

The digital preservation activities in this document are organized into the following five stages:

- **Initial Activities to Create a Digital Preservation Plan**
- **Activities to do Upon Ingest and File Creation**
- **Activities to do Regularly**
- **Activities to do Less Frequently**
- **Activities to do in Response to a Disaster or Emergency**.

The bulk of planning work occurs in the first stage, with implementation and management work in later stages. These steps allow you to create an outline of a digital preservation plan. Your final digital preservation plan, policies, and workflows will have much more detail and will be specific to your department or institution.

Initial Activities to Create a Digital Preservation Plan

- Meet with people in your department and institution in order to have conversations about digital preservation needs and goals from multiple perspectives. Some questions to consider:
    - What content do we want to preserve in the long term?
    - What existing resources and funds can we use for digital preservation? What resources and funds do we need to bring in?
    - Does our IT department understand our digital preservation needs? Can they meet them? Does our staff need to provide more information or support?
    - What staff members will be involved in digital preservation?
- Inventory existing digital content.
    - Make sure there is a record of any digital content you want to keep. Start with a simple inventory to make sure you have at least minimal information.
    - A simple inventory might include: file name, file type, file size, date created/modified, creator, location, and other fields.
    - Later inventories can be much more detailed, with additional preservation metadata fields like: creation hardware, timestamp, file fixity information, etc.
- Select and identify materials for digital preservation.
    - Not all digital files need to be preserved, select the highest quality files that will be preserved long term.
    - Some files might have a certain lifespan and shouldn't be preserved indefinitely.
- Plan (and purchase if needed) storage solutions that allow you to save multiple copies in multiple places on multiple formats.
    - A common strategy is the 3-2-1 Rule: 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.
- Evaluate metadata and create or enhance metadata of existing digital content. Make a metadata plan for future content, including preservation metadata.
- Assess staffing needs for digital preservation activities. Some things to consider:
    - Who is available to be involved in digital preservation activities inside your department and outside?
    - Who has expertise with technology, or is willing to learn?

    - What is the scope of digital preservation for your department? You may need less staff time if you have only a few digital collections, or more staff time if you have hundreds of digital collections with rapid growth.
    - Who might be suited to long term planning? Who might be suited to day-to-day digital preservation tasks?
- Check permissions, understand who has access to what digital files, and change permissions if necessary based on your own cultural norms and institutional goals.
- Research specific tools, equipment, and relevant policies you may want to use in your organization. Some suggestions for research include:
    - Read the Library of Congress digital preservation blog, *The Signal.*
    - Look at resources like the Community Owned Digital Preservation Tool Registry (COPTR), to learn about digital preservation tools (http://coptr.digipres.org/).
    - Follow the Digital POWRR Project (http://digitalpowrr.niu.edu/). You can find several resources from this group on the SHN, including:
        - From Theory to Action: “Good Enough” Digital Preservation Solutions for Under-Resourced Cultural Heritage Institutions
        - You’ve Got to Walk Before You Can Run: First Steps for Managing Born-Digital Content Received on Physical Media
    - Find examples. Universities and other repositories often share digital preservation policies and documentation online.
    - Find national or regional professional organizations or groups that relate to your type of institution. Professional organizations are a good place to start for finding publications, conference proceedings, and email listservs to keep up to date with advances in the field. Some examples include:
        - The National Digital Stewardship Alliance (NDSA)
        - The Association of Tribal Archives, Libraries, and Museums (ATALM)
        - Digital Preservation Outreach and Education (DPOE).
- Create plans for digital content in the case of a disaster or emergency:
    - Know what natural or human-made disasters might affect your region and create plans of what to do in response.
    - Consider hardware failures, network errors, network security and external attacks, software failure, media failure, and/or obsolescence.
    - When will fixity be checked? If there is a problem with files after a disaster event, how will files be restored?

Activities to do Upon Ingest and File Creation

When the planning activities within the previous stage are complete, this stage of activities will help you work with new digital content. Your institution might accept new digital content as donations or create new digital content through digitization projects.

- Add information about new digital content to a digital materials inventory.
    - This information can be added to a simple inventory that covers all digital content, or you can create an inventory for each digital collection.
    - Decide what level of detail and method of documentation is best for your institution, and be consistent.
    - Possible fields include: file name, file type, file size, date created/modified, creator, location, and additional preservation metadata fields like creation hardware, timestamp, file fixity information, etc.
- Save master preservation file and create access file or other derivative files.
- Capture and create metadata.
- Run fixity check (either compare against provided fixity information or create new fixity information).
- Run virus checks on new files (coming from outside your organization) to ensure the safety of files and systems.
- Use a write blocker when ingesting files from outside your organization to ensure authenticity.
- Migrate proprietary file formats to open source file formats.
- Determine hardware and software necessary for accessing files.

Activities to do Regularly

- Update software.
- Run virus checks on computers.
- Run fixity checks in a consistent schedule.
- Backup files on a regular basis.
- Migrate obsolete file formats.

Activities to do Less Frequently

- Research new tools, equipment, or procedures that you may want to use in your organization.
- Update storage media according to the lifespan of the media recommended by the manufacturer. Have a procedure in place so you are aware of when storage media will be likely to fail.
    - For example, external hard drives should be replaced every 3-5 years.
- Review digital preservation policy and revise as needed. Write a revision date into your policy.

Activities to do in Response to Disaster or Emergency

- Follow your digital disaster or emergency plan (assuming you have created one as part of your overall digital preservation plan).
- Assess what loss or damage has occurred by running fixity checks, checking inventories, and other methods.
- Retrieve all possible content from your backup systems and restore files as needed.
- Assess the effectiveness of your disaster/emergency plan and revise as needed.