MANAGING DIGITAL CONTENT OVER TIME

Part 4. Protect
Identify - what digital content do you have?
Select - what portion of that content will be preserved?
Store - what issues are there for long term storage?
Protect - what steps are needed to protect your digital content?
Manage - what provisions are needed for long-term management?
Provide - what considerations are there for long-term access?
OUTLINE OF “PROTECT” DISCUSSION

A. What are we protecting from?
B. Everyday protection
C. Planning for and implementing protection program
D. Basic disaster planning
A. WHAT ARE WE PROTECTING CONTENT FROM?

- Institutional support
- Human intervention
- File corruption
- Computer failure
- Misplaced metadata
- Natural disaster
- File format obsolescence
B. EVERYDAY PROTECTION

- Know where your content is located
  - Onsite and offsite; online and offline
**EASY STEPS YOU CAN TAKE**

- Put copies on different networked servers
- Swap data with a friend
- Take a copy of your data home

*Set up mechanisms to make this an ongoing process.*
Define who can access to your data
- DP staff, IT staff, patrons, interns, colleagues, other?
  - Or, just you?
EASY STEPS YOU CAN TAKE

- Store a copy of your master files offsite (at home?)
- Change the access controls on the directory in which your master files are stored so only you (and one other person) can change them
  - Microsoft support: [http://support.microsoft.com/kb/308419#4](http://support.microsoft.com/kb/308419#4)
- Bury your master file directories in the network (but leave a breadcrumb document that another person knows about)
  - Make your **access** files easily available for colleagues to find & use
B. EVERYDAY PROTECTION

Manage authentication information
- Archives community calls it “Provenance”
- IT calls it “Audit trail”

Authentication means proving, through documentation, the event history of your files
- Creation date and creator
- Modified date and modifier
- Migration date and new format
- Keeping related files related
TRACKING THE HISTORY OF YOUR DIGITAL FILES

File created by Amy R. on March 15, 2012
File emailed to Jody DeRidder on March 17, 2012
File edited by Jody DeRidder on March 18, 2012
File emailed to Amy R. on March 19, 2012
File finalized and saved on server March 20, 2012
INTERMEDIARY STEPS YOU CAN TAKE

- **Documentation**
  - Create a general document that explains your file **management workflows**. Keep a copy of that document with your files.
  - Create (perhaps in the same document) a table that contains information any time you perform **collection-wide actions**
    - File renaming
    - Format migration
    - Etc.
  - Ensure that your **metadata is well formed**, correct, and that it always “travels” with your files.
B. EVERYDAY PROTECTION

- Track and review usage, adjust practices, rinse, and repeat
  - Who is using and how is content being used in-house?
  - How is your content being used on the web?
  - Can usage information inform what else in your collection needs focused care?

Google analytics (http://www.google.com/analytics/)
EASY STEPS YOU CAN TAKE

- Track usage automatically
  - Google docs?
- Track usage manually
  - Keep a folder of requests for usage
  - Document usage in other ways...
- Use what you learn for decision making
  - What else should you focus your preservation efforts on?

User feedback:

- NCpedia best comment of the month or email:
  "Dude!!! Because of this awesome stuff I didn’t fall social studies!! ROCK ON BROTHERS!!!!!!!
  "http://ncpedia.org/transportation/overview/1926#comment-5234

"I just saw a coyote yesterday (1/28/2012) just outside of Mebane. I was watching my small dog in our backyard
from a window when the coyote trotted by into the tree line behind our house. It was thrilling to see it, but I quickly
ran outside and brought my dog. From what I’ve read on the internet they are very opportunistic and are not a
threat to people." http://ncpedia.org/wildlife/coyotecomment-1018

- Digital collections best comment or email of the month:
  - "I love this!! I’m his GGG Grandson, John William Morton, Jr."

- From an agency staff member regarding our ongoing digitization of her requests:
  - "On behalf of the State Center, I want to thank you for providing us such quick turn-around on our request.
    I really appreciate the partnership we have established with the State Library. I believe you are one of the
    state’s true gems."

- From a research librarian at a law firm regarding Session Laws online:
  - "Thanks Kathleen! You guys have done a monumental job, by the way. It’s really great to know that
    these things are online."

- # reference questions:
  - NCStats: 27 hours monitored.
  - Total inquiries through digital collections: 21
    - 13 answered
    - 8 forwarded
  - Answered: 5 questions
C. PLANNING FOR & IMPLEMENTING A DIGITAL PRESERVATION PROGRAM

- Readiness: Protect your investment in your digital content
  - Being prepared is good practice, and saves time and money
    - Digital preservation policies & plans
    - Disaster plans must include digital resources
  - Realize and fix gaps before something unwanted happens
    - Gap analysis
C. PLANNING FOR & IMPLEMENTING A DIGITAL PRESERVATION PROGRAM: READINESS

- Proper planning should allow you to:
  - **Prevent** – undesirable outcomes
  - **Predict** – most likely risks and threats
  - **Detect** – errors, problems, damage
  - **Respond** – with appropriate measures
  - **Repair** – damage or possible loss

---

*Flash floods in June 2006 hit the City Assessor’s Office in Oneonta, NY. Photo: Mario R. Arevalo, Oneonta (NY) City Assessor.*
C. PLANNING FOR & IMPLEMENTING A DIGITAL PRESERVATION PROGRAM

- Risk Management
  - Identify possible risks
  - Define those risks (nature and scope)
  - Assess potential impact (possible damage)
  - Develop appropriate, feasible responses (plans)
  - Respond to risks, threats (implement plans)
C. PLANNING FOR & IMPLEMENTING A DIGITAL PRESERVATION PROGRAM

- Emergency protection
  - What does your disaster plan say now about digital preservation?
  - What should it say?

- Who do you need to include in digital preservation planning decisions? How do you get to the hearts & minds of other staff?
C. PLANNING FOR & IMPLEMENTING A DP PROGRAM: EMERGENCY PROTECTION

- Engage in ongoing disaster planning
  - Establish committee and share information
  - Develop and maintain documents
  - Make them publicly available
    - Put them somewhere you can access them in case of an emergency
    - Put them somewhere else, too.
    - And, then copy them again. *Really.*

- Identify possible outcomes and prepare
  - e.g., what do you do when the server goes down or media is damaged?
D. BASIC DISASTER PLANNING

SAFETY OF EMPLOYEES AND GUESTS COMES FIRST!

Photo showing collapsed library shelving in the 2010 magnitude-7.1 Canterbury New Zealand Earthquake (Photo courtesy of University of Canterbury).
D. BASIC DISASTER PLANNING: WHAT NEEDS TO BE AVAILABLE SOONEST?

1. Identify core functions as part of planning
   - **Administrative**: personnel & budget data, AUL/library director
   - **Back-end systems**: network security, redundant storage/networks, staff directories, preservation/archival systems
   - **Public web access**: website, library catalog, other CMSs, wireless
   - **Public computing**: workstations, printers, etc.
   - **Security systems**: alarm systems, security cameras, etc.

2. Determine allowable downtime for each
   - **Be realistic...people have families and homes that take priority**
D. BASIC DISASTER PLANNING

3. Consider steps to re-establish each function
   - Who is responsible? How are they responsible? What is required?

4. Develop relevant documents

5. Make sure planning documents are accessible
   - On- and off-site; Lots of copies...

[http://www.dplan.org](http://www.dplan.org)
INSTITUTIONAL ASSESSMENT / AUDIT TOOLS

- Audit and certification of trustworthy digital repositories
  - [http://public.ccsds.org/publications/archive/652x0m1.pdf](http://public.ccsds.org/publications/archive/652x0m1.pdf)

- Digital Preservation Readiness Assessment: Guide for Clients

- Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) toolkit
  - [http://www.repositoryaudit.eu/](http://www.repositoryaudit.eu/)

- Planning for Digital Preservation: A Self-Assessment Tool

- Trustworthy Digital Repositories Audit & Certification (TDR)
DISASTER PLANNING RESOURCES
DIGITAL PRESERVATION POLICIES

- Columbia University. 2006.
  - [http://library.columbia.edu/services/preservation/dlpolicy.html](http://library.columbia.edu/services/preservation/dlpolicy.html)

  - [http://hdl.handle.net/1813/11230](http://hdl.handle.net/1813/11230)

- IDEALS Digital Preservation Policy. 2009
  - [https://services.ideals.illinois.edu/wiki/bin/view/IDEALS/IDEALSDigitalPreservationPolicy](https://services.ideals.illinois.edu/wiki/bin/view/IDEALS/IDEALSDigitalPreservationPolicy)