Digital Asset Protection

ALLIANCE FOR RESPONSE – CONCURRENT SESSION
APRIL 27, 2016

Elizabeth La Beaud, MLIS, DAS
DIGITAL LAB MANAGER, THE UNIVERSITY OF SOUTHERN MISSISSIPPI
Roadmap

• Definitions
• Digital Preservation Fundamentals
• Common Preparedness Actions
• Disaster Specific Concerns

Deliverables

• Define and identify your digital assets
• Identify multiple risks to digital assets
• Walk away with at least 1 actionable item to improve your digital asset protection strategy.
What is Digital Asset Management?

**DIGITAL ASSET MANAGEMENT**

- Systems designed to organize and display digital content produced in a variety of media types. The content is usually locally owned and controlled, rather than licensed from a third party.

**ELECTRONIC RESOURCE MANAGEMENT**

- Systems developed to assist librarians in the control of licensed third-party resources published electronically (databases, e-books, e-journals, etc.)

Examples of Digital Assets

- Digitized photographs
- Word Documents
- Video
- Email
- Websites
Risks to Digital Assets
A Sampling...

- Software obsolescence
- Loss of power
- Bit rot
- Hardware failure
- Cyber attacks
- Format obsolescence
- Media failure or obsolescence
- Man-made and natural disasters
- Dust
- User error

Questions to consider...

- Is the equipment needed to access your assets covered in your insurance plan?
- If your office lost power, could you access your needed files?
- If your desktop disappeared, could you access your needed files?
- If the fire alarm went off, could you leave without stopping to retrieve your server?
Levels of Digital Preservation

NDSA

Storage & Geographic Location

<table>
<thead>
<tr>
<th>Storage and Geographic Location</th>
<th>- Two complete copies that are not collocated</th>
<th>- At least three complete copies</th>
<th>- At least one copy in a different geographic location</th>
<th>- At least one copy in a geographic location with a different disaster threat</th>
<th>- At least three copies in geographic locations with different disaster threats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- For data on heterogeneous media (optical discs, hard drives, etc.) get the content off the medium and into your storage system</td>
<td>- Document your storage system(s) and storage media and what you need to use them</td>
<td>- Obsolescence monitoring process for your storage system(s) and media</td>
<td>- Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems</td>
<td></td>
</tr>
</tbody>
</table>
Storage

- Solid State Drives
- Hard Drives
- Optical
- Magnetic

Storage Trends

Tape → Optical → Solid State → Cloud
Why CDs are NOT long term storage...

Storage Trends

Tape → Optical → Solid State → Cloud
Cloud

- Vendor hosted
- Where is your data?
- What happens if your vendor goes out of business...what happens to your data?
- If you don't know, call your vendor and check your contract.

Where the cloud really is...
Amazon Web Services

File Fixity & Data Integrity

<table>
<thead>
<tr>
<th>File Fixity and Data Integrity</th>
<th>- Check file fixity on ingest if it has been provided with the content.</th>
<th>- Check fixity on all ingests.</th>
<th>- Check fixity of content at fixed intervals.</th>
<th>- Check fixity of all content in response to specific events or activities.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Use write-blockers when working with original media.</td>
<td>- Maintain logs of fixity info; supply audit on demand.</td>
<td>- Ability to detect corrupt data.</td>
<td>- Ability to replace/repair corrupted data.</td>
</tr>
<tr>
<td></td>
<td>- Virus-check high risk content.</td>
<td>- Supply audit on demand.</td>
<td>- Virus-check all content.</td>
<td>- Ensure no one person has write access to all copies.</td>
</tr>
</tbody>
</table>
Cryptographic Hashes

- Checksums
  - SHA256
  - MD5
- MD5 Summer
- AVPreserve's Fixity
- File Verifier ++
  - (these are windows examples)

Information Security

<table>
<thead>
<tr>
<th>Information Security</th>
<th>Identify who has read, write, move and delete authorisation to individual files</th>
<th>Document access restrictions for content</th>
<th>Maintain logs of who performed what actions on files, including deletions and preservation actions</th>
<th>Perform audit of logs</th>
</tr>
</thead>
</table>

Information Security

• Make sure no one person has write privileges to all copies.

Metadata

<table>
<thead>
<tr>
<th>Metadata</th>
<th>- Inventory of content and its storage location</th>
<th>- Store administrative metadata</th>
<th>- Store standard technical and descriptive metadata</th>
<th>- Store standard preservation metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Ensure backup and non-collocation of inventory</td>
<td>- Store transformative metadata and log events</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Metadata
- Descriptive Metadata
- Dublin Core
- Mods
- Technical Metadata
- MIX
- Structural Metadata
- METS
- Preservation Metadata
- PREMIS

File Format Sustainability
File Format Sustainability

- Disclosure
- Adoption
- Transparency
- Self-documentation
- External dependencies
- Impact of patents
- Technical protection mechanisms

File Naming Conventions

- No spaces
- Avoid special characters
- Consistent date format
  - YYYY-MM-DD
What would you do in the event of...

- A power outage?
- A flood or leak?
- A fire?
- A tornado?
- A hurricane?
- An earthquake?
- A volcano?

Action List Ideas

- Non co-location of inventory
- Call insurance company to see if vital equipment is covered
- Call vendor to see where your data is stored and what happens to it if vendor goes out of business
- Pick computers off the floor
- Purchase UPS
- Replicate data offsite
- Migrate files to sustainable formats
- Adopt sustainable file naming conventions
- Create list of operational needs
- Add digital assets into Disaster Recovery Plan
Further Reading...

• Levels of Digital Preservation

• File naming conventions
  http://guides.lib.purdue.edu/c.php?g=353013&p=2378293

• Benefits and risks of PDF/A-3
  http://lcweb2.loc.gov/master/gdc/lcpubs/2013655115.pdf

• Hathitrust Disaster Recovery Plan
  http://lcweb2.loc.gov/master/gdc/lcpubs/2013655115.pdf

Questions?