TABLE OF CONTENTS

INTRODUCTION

Purpose

We at the Paul V. Galvin Library recognize that effective disaster planning is essential for ensuring the safety of our staff and the sustainability of our digital collection content and services. We also recognize that disaster preparedness is one of our primary responsibilities as stewards of a trusted digital repository. **The purpose of this plan is to sustain continued preservation of the digital assets that have been entrusted to the library, as well as our supporting systems, through preparation, planning, and developed recovery scenarios.** This plan is intended to communicate to IIT staff the guiding disaster preparedness principles, policies, and recovery plans for our digital assets and services for the benefit of our depositors, funders, and users.

Scope

This plan focuses on 1) the long-term preservation of the digital collections and their related metadata hosted by the library. This includes: share.iit.edu, Illinois Institute of Technology's institutional repository; digital collections hosted by the library; and other digital files and records maintained by the library. 2) This plan also focuses on disaster recovery for our supporting systems and other digital services. This plan is meant to complement other disaster plans created by the Illinois Institute of Technology and the Paul V. Galvin Library that focus on evacuation procedures, patron safety, and disaster recovery of the library's physical collection.

Commitment

This plan reflects Galvin's commitment to its mission statement in the event of a small- or large-scale digital disaster and helps ensure the sustainability of a digital preservation program. The policies and recommendations of this document comply with prevailing standards and practices of the digital curation community.

It is recommended that the library further its commitment to preserving its digital assets and services by including digital preservation in its mission statement and setting aside funds for digital preservation in the budget.

How this Document is Organized

This plan is organized into three sections: 1) disaster preparedness and mitigation, 2) digital disaster recovery, and 3) the appendices. *Disaster preparedness and mitigation* focuses on the ongoing actions that take place to mitigate risk of data or service loss and that ultimately ensure the long-term preservation of critical digital assets and their supporting systems. *Digital disaster recovery* focuses on the actions that take place in the event of a small- or large-scale disaster. The former is proactive, the latter reactive. Finally, the appendices include contact information, resources, and other relevant documents.

This plan also includes specific risk recommendations that have been highlighted in orange.

Notes

This document was prepared by Heidi Uphoff, a practicum student from the University of Illinois, and Dana Lamparello, the library's Digitization and Metadata Librarian. ***This document is intended to be a template and a recommendation*** to be periodically edited by staff at the library and added to the library's suite of disaster plans. It was last updated September 5, 2012.

DISASTER PREPAREDNESS AND MITIGATION

Definition of Disaster Mitigation and Purpose of this Section

Disaster mitigation is defined as all activities undertaken to ensure the long-term preservation of digital assets and their supporting systems and to reduce data loss and corruption during a disaster. These activities are implemented through a cycle of planning, training, equipping, and evaluation to correct deficiencies and to mitigate vulnerabilities. The purpose of this section is to describe the preparedness activities undertaken by the library.

Digital Preservation Planning Principles

- The library will maintain multiple copies of digital collection content (data, documentation, metadata, and associated materials) in digital form.
- At least one copy of the digital collection content will be stored offline on tape media or with a cloud storage company as a failsafe copy.
- The library will provide guidelines for acceptable digital formats and minimal-level metadata necessary for long-term storage and preservation.
- The library will monitor changes in the technology environment to manage risk as technology evolves and to provide continuing access and updated methods of access as necessary, such as migrating digital content to new formats or providing system emulators to access original formats.
- All servers and computers will be protected by the latest anti-virus software and security patches.

These principles reflect the current state of digital preservation at the library and do not reflect the best practices of the data curation community. It is recommended that six copies of digital objects are kept on and off-site. A complete list of recommendations for improving these principles can be found at the end of this section in "risk assessment recommendations."

Formats

The library chooses well-supported, stable, open standard file formats for which good documentation is available for and for which a variety of access tools are expected to remain available into the future.

Migration

While DSpace as a software platform can accept and store all file formats, the Galvin Library agrees to fully support only those well-documented and most widely used). Galvin Library therefore reserves the rights to migrate undocumented and uncommon file formats to stable preservation formats when necessary.

Roles and Responsibilities

The management and implementation of this plan falls under the responsibility of two groups: **The Digital Preservation Committee** and the **Digital Disaster Recovery Team**.

Digital Preservation Committee

Purpose and Goal

The purpose and goal of the **Digital Preservation Committee** is to carry out the necessary tasks to mitigate the loss and corruption of library digital assets now and in the future. They are responsible for monitoring the long-term maintenance of the digital assets created by the library and/or hosted by the library on behalf of the depositors and for the benefit of current and future users.

Committee Members

The Digital Preservation Committee consists of four standing members and one to two other members appointed for two-year terms, including at least one member from archives. The standing members are the *Systems Librarian,* the *Metadata and Digitization Librarian,* the *Head of Collection Development,* and the *Head of Reference and Resource Sharing.*

Responsibilities

In order to achieve their goals, the **Digital Preservation Committee** will:

- Review the library's relevant policies and procedures (including this document) annually to ensure they reflect the best practices recommended by the digital preservation community.
- Monitor changes in the technology environment to manage risk as technology evolves, providing continuing access and updated methods of access as necessary.
- Implement and monitor backup routines and on-going preventative strategies.
- Ensure in-house capabilities for data management and recovery are in place.
- Maintain information on levels of server storage space.
- Retain records of any situation of data loss or corruption that required backup recovery.
- Confirm that Library Technology Group student workers and other relevant personnel have been trained on backup and recovery procedures.
- Recommend to the Dean of Libraries any needed remedial actions regarding potential threats to critical data.
- Promote digital preservation awareness among library staff.

Digital Disaster Recovery Team

Purpose and Goal

The purpose and goal of the **Digital Disaster Recovery Team** is to provide leadership and immediate action required during a crisis situation so that losses are mitigated and normal operations are resumed as quickly as possible. During a medium- or large-scale disaster, the **Digital Disaster Recovery Team** acts as a sub-group for the library's general Disaster Recovery Team.

Committee Members

The **Digital Disaster Recovery team** consists of three standing members and one appointed member from the library's general Disaster Response Team to serve on two-year terms. The standing members are the *Systems Librarian,* the *Metadata and Digitization Librarian*, and the *Systems Support Specialist.* One standing member of the Digital Disaster Recovery team will be appointed by the team to serve on the library's general Disaster Response Team for two-year terms at a time. Action may not be required of all committee members in the event of a small-scale disaster.

Responsibilities

In the event of a **small-scale disaster**, which is defined as a disaster that causes short-term loss of data or interruption of services and can be recovered by in-house personnel in a timely manner without purchasing new equipment, the *Systems Support Specialist*, the *Systems Librarian,* and the *Digitization and Metadata Librarian* will:

- Notify the appropriate staff members that an issue has been identified.
- Follow the developed recovery scenarios, or create new methods as necessary, to recover the data.
- Check to ensure digital objects have been recovered completely without corruption.
- Document the issue where appropriate staff can access the information.
- Inform appropriate staff members that the data has been recovered and services have been resumed.
- Communicate with the university's community about service availability and digital content access as necessary.
- Keep a physical and digital copy of this plan in an accessible place.

In the event of **medium- or large-scale disaster**, the Digital Disaster Recovery Team will:

- Assess the crisis and decide on the appropriate response.
- Communicate with the library's Disaster Response Team the nature and status of the interruption to services.
- Coordinate as appropriate with the Disaster Response Team to carry out recovery.

- Make recommendations to Dean of Libraries when funds or additional staff is necessary to assist with response and recovery of data and supporting systems.
- Make recommendations to Disaster Response Team when outside departments, consultants, and contractors are required to carry out recovery.
- Make recommendations to Disaster Response team for the purchase of supplies and equipment as necessary.
- Make recommendations to Dean of Libraries for off-site hosting of digital assets and off-site services if needed.
- Document damage of computer and electronic equipment by written inventory and visual descriptions for insurance claim (see IIT General Counsel's policies, most specifically the Insurance Claim Filing Procedures: http://www.iit.edu/general_counsel/policies/pdfs/procedure_e1_insurance_claims_filing_procedure.pdf and Equipment Losses Procedures: http://www.iit.edu/general_counsel/policies/pdfs/procedure_e2_equipment_losses.pdf) .
- Keep a physical and digital copy of this plan in a physically and electronically accessible location.
- Review the policies and procedures of this plan annually and update as necessary.

Inventory of Digital Assets and Supporting Systems

This inventory is broken up into two groups: 1) **critical digital assets** and 2) **supporting systems**. The **critical digital asset** list consists of digital data or content hosted by library servers. The **supporting systems** list consists of systems that support the management, access, and preservation of the library's critical digital assets, as well as any digital content hosted off-site by other organizations (and thus not the primary responsibility of the library) to ensure its maintenance and preservation.

Critical Assets

- Share.iit (mix of born-digital and digitized assets): share.iit.edu
- Voices of the Holocaust (digitized assets): voices.iit.edu
- Contrails (digitized assets): contrails.iit.edu
- Tech News Collection (mix of born-digital and digitized assets): http://archives.iit.edu/technews/
- World's Columbian Exposition of 1893 (digitized assets): http://columbus.gl.iit.edu/
- Re:Discovery archival collections management system (metadata and few digitized assets)
- Library Website: library.iit.edu
- When a digital asset management system is implemented, Contrails, Tech News Collection, and World's Columbian Exposition of 1893 digital collections will likely be imported; the separate websites will cease being an access point to the collections.

Supporting Systems

- Library Technology Group (LTG) Wiki
- Network Drives
- Hardware and electronic equipment
- Computers with ability to access the internet and run key applications
- Access to the Illinois Institute of Technology's Network – hosted by the Office of Technology Services (OTS)
- Electronic library signs
- Personnel
- Internet Archive Collection – hosted by the Internet Archives and the Consortium of Academic and Research Libraries in Illinois (CARLI)
- Circulation System – hosted by CARLI
- Cataloging System – hosted by CARLI
- E-Books and Databases – hosted by off-site vendors, overseen by the *Head of Collection Development*

Location

The servers are stored in a secure room located on the lower level of the library. The servers have 4+ hours of backup reserve power from batteries to provide uninterrupted service automatically during a power outage. The battery backup system is enabled to communicate with the servers and make them shut down safely if they detect a power outage and low remaining battery. The servers shut themselves down automatically in the event of overheating or other extraneous activities that may occur. Servers are protected from disc failure via mechanical redundancy in the form of RAID configurations along with magnetic or cloud backups.

The *Library Technology Group (LTG)* keeps an updated inventory of the server room and the contents of each server on the LTG wiki (http://galvinlibrary.iit.edu/doku.php).

Volume

LTG and the *Digital Preservation Committee* monitor the storage volume of the servers.

Backup Routines

All of the library servers, except for the DSpace server, are backed up weekly by tape. These tapes are picked up once a week by Archive America and taken to an off-site storage facility in Tinley Park, IL.

The DSpace server is backed up through Amazon S3, a cloud storage service, differentially every night and totally once a month.

The *Systems Librarian,* the *Systems Support Specialist,* and all student workers are trained on the back up routines.

Risk Assessment Recommendations

- Conduct tests annually to demonstrate that digital content can be restored from backups as needed.
- Monitor the repository's media for possible degradation and subsequent integrity checking on refreshed byte streams by a system of checksums. Dspace can be programmed to do this task automatically.
- Adopt an environmental control monitoring system for the server room.
- Install an uninterrupted power supply to the server room.
- Arrange for a stable and constant environment in the library.
- Use Share.iit as a dark archive for master copies of the Colombian Exposition, Contrails, and the Tech News collections.
- Look into DuraCloud and LOCKSS as a way to maintain at least six copies of digital objects.
- Investigate the possibility of an additional server to copy data and mirror discs.
- Develop a business continuity plan in the event of a physical or digital disaster that includes off-site services, and/or off-line manuals for departments. This may include an agreement with an internal or external facility (such as CARLI or a commercially leased facility) to host our digital data in the event of a physical disaster in the server room.
- Do fixity checks and virus scans prior to a digital object's ingest into Dspace and after ingest.
- Develop training plans and policies for data storage and recovery.
- Keep multiple physical and digital copies of this plan and all disaster documents in safe and accessible places.
- Create diagrams that show which computers are associated with which networks and peripheral equipment to distinguish between those run by OTS and those that are the responsibility of LTG.

DIGITAL DISASTER RECOVERY

Definition of Digital Disaster Recovery and Purpose of this Section

Digital disaster recovery is defined as all activities designed to restore critical data, their supporting systems, and other digital services after a disaster. The purpose of this section is to detail the steps the library will undertake to restore its digital assets, their supporting systems, and other digital services to full functionality after an emergency or disaster scenario.

Prioritization for Recovery Checklist

This list of recovery priorities for digital assets and supporting systems was created using the library's mission statement, the library's collection development policy, the archives mission statement, the archives collecting scope, and the library's general disaster plan as guidelines.

Priority decisions are based on a number of ***preservation*** considerations:

- Is it unique to the library?
- Is it born digital?
- Is it available through another institution?
- Is it available in a different format at the library?
- Can it be replaced? At what cost?
- How important are these items to the collection?
- Does the content support the mission of the library or the university?

Priority decisions are based on a number of ***service*** considerations:

- Is it necessary for continuing or restoring library operations?
- Are there legal requirements for maintaining service?
- Does the service support the mission of the library or the university?

First priority

- Library website
- Proxy server

Second priority

- Data integrity of digital objects and metadata in share.iit
- When DAMS is implemented – Data integrity of digital objects and metadata in DAMS

Third priority

- Computer services, hardware, software, data
- Network drives
- Public access to Share.iit
- Re:Discovery data integrity and public access
- When DAMS is implemented – Public access to DAMS

Fourth Priority

- Voices of the Holocaust

- World's Columbian Exposition of 1893
- Contrails
- Tech News Collection
- Electronic library signs

  NOTE: World's Columbian Exposition of 1893, Contrails, Tech News digital collections will likely be consolidated and imported to the DAMS once it is implemented; these collections will then be addressed as a second and third priority above.

Recovery Scenarios

The following recovery scenarios are intended to be guidelines for recovery during specific types of disasters. The *Digital Disaster Recovery Team* may create new methods as necessary to recover the data.

Server shutdown

After any incident in which a server has been shutdown, the following steps should be taken:

1. *LTG* will determine the cause of the shutdown
    a. If caused by a prolonged power-outage and servers shut themselves down safely, *LTG* will restart the servers
    b. If caused by overheating, *LTG* will allow the server to cool and take steps to bring the environment of the server room back to an appropriate level before restarting the server
    c. If the cause is unknown, *LTG* will take steps to identify the cause and make sure it is safe before restarting the server
2. *LTG* will restart the server and check for errors and missing files
    a. If *LTG* notices a difference in file sizes, *LTG* will run a DIFF to identify what is missing
    b. *LTG* will return missing files, items, metadata, etc… whenever necessary
    c. Only when file sizes match and all errors have been fixed will *LTG* notify the *Metadata and Digitization Librarian* about complete restoration of services
    d. If it is not possible to correct the problems caused by the server shut-down, *LTG* will restore data through backup tapes or cloud storage
3. The *Metadata and Digitization Librarian* will check for errors on the client-side depending on the data stored on the server.
4. The *Metadata and Digitization Librarian* will notify *LTG* about any missing content or errors she encounters
5. Once all problems are successfully resolved, the *Digital Preservation Committee* will be notified of the restoration of services and a notice will be posted in the Library News Blog about resuming use
6. The *Digital Preservation Committee* will document this issue

Software Update to DSpace

After upgrading any component of Galvin Library's DSpace instance, Share.iit, the following steps should be taken:

1. *LTG* will compare Share.iit's upgraded file size to the backup copy created directly before upgrade.
    a. If file sizes are different, *LTG* will run a DIFF to identify what is missing
    b. *LTG* will return missing files, items, metadata, etc… whenever necessary

c. Only when file sizes match will *LTG* notify the *Metadata and Digitization Librarian* about completed upgrade.
d. If it is not possible to correct the problems caused by the upgrade, the system will be rolled back to its pre-upgrade condition

2. The *Metadata and Digitization Librarian* will check for errors on the client-side by:
    a. Logging in
    b. Ingest a test item in a collection
    c. Perform keyword searches and all browse categories on ingested test item
    d. Confirm all Share.iit customizations are intact:
        i. Homepage
            1. Community and Collection Guidelines, etc. links
            2. Learn about Share.iit link (linked to Research Guide)
        ii. Browse
            1. Department
        iii. Discover
            1. 5 results for each
            2. Only 1 listed for "Recently Added"
        iv. Advanced Search
            1. Added filters: Department, Type, IPRO Track
        v. Item Page
            1. Type field added to simple item record (didn't population in 1.7.1)
        vi. Custom workflows
            1. IPRO custom
            2. Theses
            3. Masters Projects
            4. Studios
            5. Patents
        vii. License
            1. Breadcrumbs read "Release"
            2. Two "Release" steps at end
                a. Creative Commons (links out and back into Share.iit)
                b. IIT Distribution License (IIT language / includes link to print)
        viii. Statistics
        ix. Email subscriptions to collections
            1. Chron job to run nightly
    e. *Metadata and Digitization Librarian* will notify *LTG* about any missing content or errors she encounters
    f. Once all problems are successfully resolved, the *Digital Preservation Committee* will be notified of upgrade completion and a notice will be posted in the Library News Blog about resuming use

The following are DSpace upgrade resources that may be useful:

-Upgrading a DSpace Installation
https://wiki.duraspace.org/display/DSDOC18/Upgrading+a+DSpace+Installation
-LTG DSpace documentation on Galvin Wiki
http://galvinlibrary.iit.edu/doku.php?id=Itg:dspace

Data Recovery from Magnetic Tape Backups

It is recommended that LTG develops a recovery scenario for data recovery from magnetic tapes.

Data Recovery from Cloud Storage Backups

It is recommended that LTG develops a recovery scenario for data recovery from cloud storage backups.

Storage and Basic Treatments for Materials

NOTE: All library physical assets are insured by the university; follow the insurance claim procedures outlined by General Counsel in the event of physical damage to any physical assets in the library: http://www.iit.edu/general_counsel/policies/.

Magnetic Tapes

Storage
Magnetic tape includes computer, audio, and video tapes, as well as diskettes, flash drives, SD memory cards, and other removable data storage devices. Magnetic tapes are sensitive to changes in the environment. The life span for much of this material is approximately ten years. Poor storage and environmental conditions accelerate the deterioration of the tape and its magnetic signal.

The optimum environment for magnetic media is 50º to 60º Fahrenheit with a maximum of 30% - 40% relative humidity. If this environment cannot be achieved, then strive for standard working conditions of 68º – 70º Fahrenheit with a maximum of 50% - 55% relative humidity. Relative humidity should not drop below 30%. A stable, constant environment is best.

High temperature and humidity cause distortion of sound, data, and image. High temperatures can cause sticking when winding and rewinding and encourage layer-to-layer adhesion. High humidity encourages the deterioration of the binder layer, shedding of the signal or emulsion layer, and clogging of equipment when the tape layers flake off. Low temperatures can also cause damage by loosening the spools and changing the dimensions of the tapes, causing distortion and timing errors. Low humidity encourages the attraction of debris and dust particles to tape, increases, static electricity on tapes and in machines, and inhibits playing of tapes.

Disaster Recovery
Magnetic tape is extremely sensitive to heat. Tapes distort and then become unreadable at 125º Fahrenheit. Mold and mildew eat away the binder layer, obstructing the readability of magnetic signals and distorting images or signals on the tape. *Appendix D* lists disaster recovery companies.

If not wet:
- Remove from disaster area
- Place in a dry, clean, water sealed box.

If unique and wet:
- Remove from water
- Treat immediately
- Send to professional company for drying, cleaning, and copying

If unique and exposed to dust, soot, or particulate matter:

- Remove from disaster area
- Dry first and then clean
- Send to professional company for drying, cleaning, and copying

CAUTION: Never run a damaged or wet tape on a regular tape drive

CAUTION: Never let a wet tape drive on its own, it will adhere to whatever it touches, resulting in permanent loss of sound, image, or data.

Optical Discs

Storage
Optical discs include CDs, DVDs, and other optical storage devices in all their formats. Optical discs are fairly stable and, for the most part, will remain unaffected by normal temperatures. For longevity and seldom-used collections, optimal or ideal environment conditions are 68º Fahrenheit and 45% relative humidity. It is best to keep the temperature and relative humidity stable. Fluctuations in temperature could cause the polycarbonate to crack. Avoid freezing optical discs or subjecting them to dramatic changes in temperature. Optical discs are also susceptible to high temperatures as the polycarbonate may soften at 212º Fahrenheit. Avoid exposing optical discs to particulate matter and pollution as they can inhibit the signal and erode the polycarbonate. Avoid storing them near solvents such as janitorial supplies, ozone, and paint, all of which can corrode the polycarbonate.

Disaster Recovery
Optical Discs are susceptible to water, mold, and mildew.

If not wet:

- Remove from disaster area
- Store in a dry, clean, pollution- and particulate- free environment.

If wet:

- Remove from water
- Open, check for and drain any water that may have entered the case or container
- Remove the disk from any paper jacket or plastic case
- Retain or replace labeling
- Allow it to dry for 48 hours
- Store in a dry, clean, pollution- and particulate- free environment.

If exposed to dust, soot, or particulate matter:

- Remove from disaster area

- Clean dirt, ash, and smoke residue from containers and/or sleeves
- Remove the disc and wipe any debris from the inside of the case
- Carefully wipe the debris from the optical disk from the center of the disc outward to the edge (radically) and not in a circular motion around the disc (concentrically)
- Allow it to dry for 48 hours
- Store in a dry, clean, pollution- and particulate- free environment.

CAUTION: Always use a dry, lint-free cotton cloth to clean discs and never spray cleaning solutions directly on discs.

Computer Equipment

Check the recovery priority for equipment and always follow-up with General Counsel about extent of insurance coverage.

If dry

- Remove to dry, safe location

If upgrade scheduled

- Replace according to needs and insurance coverage

If wet and not covered by insurance

- Open covers
- Do not let ceiling tiles, soot, and dirt drop inside
- Let inside dry
- Recertify equipment

If fire-damaged

- Open covers

If there is soot or dirt inside and not covered by insurance

- Have disaster recovery firm dry, clean, and restore and recertify equipment to pre-loss condition
- Replace parts as necessary

Succession Plan for Share.iit

One of the attributes of a trusted digital repository is organizational viability. The long-term preservation of digital objects in Share.iit is the responsibility of the Paul V. Galvin Library. If, for any reason, the library should discontinue its support of Share.iit, one of the following options will occur:

- A different department or entity within IIT will assume responsibility for Share.iit,
- The contents will be returned to the depositor(s) in an agreed upon manner
- A partner digital archive program outside of IIT will be identified and asked to assume responsibility for the content. At the time of transfer, Galvin Library will ensure that the transfer media and dissemination format will be relevant and compatible with current best practices and standards.

As the digital preservation community evolves in its understanding of digital repositories these conditions are subject to change.

It is recommended that a succession plan be created for the other digital collections once DAMS has been implemented.

APPENDIX A

CONTACT INFORMATION FOR THE DIGITAL PRESERVATION COMMITTEE

John Dorr (standing member)
Head of Reference Services
Work: 312-567-3615
Cell:
dorr@iit.edu

Paul Go (standing member)
Systems Librarian/Library Technology Manager
Work: 312-567-7997
Cell:
pgo@iit.edu

Dana Lamparello (standing member)
Metadata & Digitization Librarian
Work: 312-567-3373
Cell: [redacted]
dlampare@iit.edu

Charles Uth (standing member)
Head of Collection Development & Management
Work: 312-567-5319
Cell:
uth@iit.edu

Catherine Bruck (rotating member)
University Archivist
Work: 312.567.6840
Home:
bruck@iit.edu

Liana Khananashvili (rotating member)
Head of Bibliographic Services
Work: 312.567.6875
Cell:
khananashvili@iit.edu

APPENDIX B

CONTACT INFORMATION FOR DIGITAL DISASTER RECOVERY TEAM

Brian Bjerke (standing member)
Systems Support Specialist
Work: 312.567.8603
Cell:
bbjerke@iit.edu

Paul Go (standing member)
Systems Librarian/Library Technology Manager
Work: 312-567-7997
Cell:
pgo@iit.edu

Dana Lamparello (standing member)
Metadata & Digitization Librarian
Work: 312-567-3373
Cell: [redacted]
dlampare@iit.edu

Pattie Piotrowski (rotating member)
Assistant Dean for Public Services
Work: 312.567.3386
Cell:
piotrowski@iit.edu

APPENDIX C

CONTACT INFORMATION FOR NON-LTG SUPPORTING GROUPS

Archive America – Chicago Area Branch
8400 West 185th Street
Tinley Park, IL 60487
Phone: 1.800.273.8587
info.chicago@archiveamerica.com

CARLI – Consortium of Academic and Research Libraries in Illinois
Contact for OPAC and Internet Archive
Elizabeth Clarage
Director of Collections Services
Consortium of Academic and Research Libraries in Illinois
100 Trade Centre Dr., Ste. 303
Champaign, IL 61820
Phone: 217.300.2624
Email: clarage@uillinois.edu / support@carli.illinois.edu
http://www.carli.illinois.edu/

IIT's Department of Facilities
8:00am-5:30pm Monday-Friday Phone: 312.567.3343
After hours call public safety

IIT's Office of Technology Services
Phone: 312.567.3375
Email: supportdesk@iit.edu
NOTE: The *Digital Preservation Committee* should establish better emergency contacts at OTS other than the main support desk.

IIT's Public Safety Office
Emergency Phone: 312.808.6363
Non-Emergency Phone: 312.808.6300

APPENDIX D

VENDORS

Magnetic Tape – Cleaning and Restoration

NBD International, Inc.
P.O. Box 1003
241 Myrtle Street Ravenna, OH 44266
Phone: 330.296.0221 or 800.929.3398
Fax: 330.296.0292 or 800.783.3802
www.nbdint.com
Water- and smoke-damage recovery of audio-and videotape; computer tapes, diskettes, and CD formats; and vinyl records. Also provides water- and smoke-damage recovery of paper-based materials.

OnTrack Data International, Inc.
9023 Columbine Road
Eden Prairie, MN 55347
Phone: 952.937.5161 or 800.872.2599
Fax: 952.937.5750
www.ontrackdatarecovery.com
Magnetic media, computer tapes, hard drives, and diskettes

Tek Media Supply Company (a subsidiary of the RTI Group)
4700 Chase
Lincolnwood, IL 60712-1689
Phone: 847.677.3000 or 800.784.6733
www.rtico.com/tekmedia/
Cleaning, inspection, and repair supplies for AV: film, tapes, and discs

Contingency Planning and Response Companies with Hot or Cold Sites

IBM Corporation
1 New Orchard Road
Armonk, New York 10504-1722
Phone: 914.499.1900
IBM Business Continuity and Resiliency Services
Phone: 800.IBM.7080
http://www-935.ibm.com/services/us/en/it-services/business-continuity-and-resiliency-services.html

SunGard Availability Services
680 East Swedesford Road
Wayne, PA 19087
Phone: 800.468.7483
Alert and Disaster Hotline: 866.722.1313
www.sungardas.com

APPENSIX E

INVENTORY OF DAMAGED EQUIPMENT FORM

Documenting the damage – Create one chart per floor, room, or department

Type of Computer Component	Serial #	Type of Damage	Replace or Repair	Contracted or Internal Work	Cost (PO#) / Insurance Coverage	Date Completed

APPENDIX F

RESOURCES USED TO CREATE THIS DOCUMENT

Bishoff, Liz, and Tom Clareson. "Assessing Preservation Readiness Webinar." Lecture. *Assessing Your Preservation Readiness: A DuraSpace Webinar*. DuraSpace, 07 Feb. 2012. Web. 22 May 2012. <http://www.slideshare.net/DuraSpace/assessing-preservation-readiness-webinar>.

Cervone, H. Frank. "Disaster Recovery and Continuity Planning for Digital Library Systems." *OCLC Systems & Services* 22.3 (2006): 173-78. Web. 27 June 2012.

Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System*. 2002. Print.

dPlan: The Online Disaster-Planning Tool for Cultural and Civic Institutions. Web. 15 June 2012. <http://www.dplan.org>

ICPSR. (2012). *Disaster Planning*. Web. 20 June 2012. at http://www.icpsr.umich.edu/icpsrweb/ICPSR/curation/disaster/index.jsp

Kahn, Miriam. *Disaster Response and Planning for Libraries. 3rd ed. Chicago: American Library Association*, 2012. Print.

Kahn, Miriam. *Protecting Your Library's Digital Sources: The Essential Guide to Planning and Preservation*. Chicago: American Library Association, 2004. Print.

Mallery, Mary. "Technology Disaster Response Planning for Libraries." Lecture. NJLA Conference 2012. Web. 29 June 2012. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=9&ved=0CGkQFjAI&url=http%3A%2F%2Fnjlaconference.info%2Fsites%2Fnjlaconference.info%2Ffiles%2Ftechnology_disaster_planning_for_libraries2.pptx&ei=GwPrT-HVEqjq2QWToam3AQ&usg=AFQjCNGF17A0odm5lx-jWc9j3y4VkV2FYw&sig2=ktvQYRamws2i3TVQZxv9zA>.

"Northeast Document Conservation Center Resources: Preservation Leaflets." *Northeast Document Conservation Center Resources: Preservation Leaflets*. Web. 22 May 2012. <http://www.nedcc.org/resources/leaflets.list.php>.

Northwestern University Library Policies, by permission of Claire Stewart.

"Risk Management and Disaster Planning." *CNI: Coalition for Networked Information*. N.p., n.d. Web. 31 June 2012. <http://www.cni.org/executive-roundtable-reports/risk-management-and-disaster-planning>.

Ritzenthaler, Mary L. *Preserving Archives & Manuscripts.* 2nd ed. Chicago: Society of American Archivists, 2010. Print. Archival Fundamentals Ser. II.

RLG-OCLC Report. *Trusted Digital Repositories: Attributes and Responsibilities*. 2002. Print.

Stuchell, Lance. "Beyond Backups: Lessons Learned from Disaster Planning for a Digital Archive." Lecture. *2010 SAA Presentation Section Meeting.* 16 August 2010. Web. Accessed 15 June 2012. <http://www.slideshare.net/lancestuch/saa-disaster-planningfinal>

Swanson, Marianne, Ray Thomas, Joan Hash, Tim Grace, Lucinda Pope, and Amy Whol. *Contingency Planning Guide for Information Science Systems*. Rep. National Institute of Standards and Technology, June 2002. Web. 20 June 2012. <http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=115>.

University of California, Los Angeles. *Social Science Data Archive: Disaster Recovery Plan.* Web. 22 May 2012. <https://docs.google.com/viewer?a=v&pid=gmail&attid=0.1&thid=137046f8144ab582&mt=application/vnd.openxmlformats-officedocument.wordprocessingml.document&url=https://mail.google.com/mail/?ui%3D2%26ik%3Dd4b05f45db%26view%3Datt%26th%3D137046f8144ab582%26attid%3D0.1%26disp%3Dsafe%26realattid%3Df_h1nub8ge0%26zw&sig=AHIEtbRZA4FhosH14Y9ZKwrSSxXBEnpFYQ&pli=1>

University of Illinois – Urbana, Champaign. *Preservation and Conservation.* Web. Accessed 15 June 2012. <http://www.library.illinois.edu/prescons/disaster_response/main_library_disaster_plan/index.html> <http://www.library.illinois.edu/prescons/disaster_response/eep_flipbook/eep_handbook.html>

APPENDIX G

RELATED DOCUMENTS

Paul V. Galvin Library's Disaster Plan

- This disaster plan is for evacuation safety, building and physical collection recovery. A physical copy of this plan is located in the Administrative Assistant's office. Copies of the library's emergency evacuation procedures are located on the Common (H) drive.
- This document was created ten years ago and does not reflect the updated evacuation and emergency procedure documents located on the Common (H) drive in the "emergency" folder.

Illinois Institute of Technology's Crisis Response Plans

- http://iit.edu/about/pdfs/emergency_flip_chart_022405.pdf

Share.iit's policies

- Copies of policies and documents related to share.iit are located on the Common (H) drive and the LTG wiki.