This document summarizes the resources that ICPSR researched in the process of preparing its Disaster Plan.

**Internal (University of Michigan)**

**University of Michigan Administrative Information Services (MAIS)**

Broadly outlines the need for and function of UM Emergency Management, Business Continuity, and Disaster Recovery Planning. This site contains the Washtenaw County Hazard Ranking List, which prioritizes types of events by frequency and number of people affected. MAIS also provides templates for units to manage the planning, testing, and auditing of disaster and continuity programs.

**Provost and Executive Vice President for Academic Affairs**

This office authored the Standard Practice Guide: Institutional Data Resource Management Policy, which defines institutional data resources as University assets and makes recommendations on identifying, preserving, and providing access to these assets. ICPSR has identified its digital assets as University data resources, and is currently in line with requirements outlined by the above policy.

**Emergency Action Plan (Institute for Social Research)**

The Perry Building Emergency Action Plan (EAP) contains vital information on procedures to follow during an emergency. In addition to building-specific information such as exit maps and contact information, the plan outlines individual responsibilities in the event of a disaster; planning; evacuation procedures for fire, explosions, and hazardous materials incidents; severe weather shelter areas; bomb threats and suspicious packages; and building closings due to loss of power, gas, or water.

---

**External Resources**

**Policy Planning Tools**

**Association of Public Treasurers of the United States and Canada: Disaster Policy Certification Guidelines**

This is a planning document and template for disaster management policies, providing outlines and example language on several facets of a strong policy, including the possible loss of a building, the replacement of computer resources, and testing and training for the disaster plan. The plan also outlines the need to identify possible threats to assets, this would be useful in combination with the Washtenaw County Hazard Ranking List, contained on the MAIS Emergency Management Web page.

**Examples of Disaster Planning Policies**

**Washington State Department of Information Services: Disaster Recovery and Business Resumption Planning Policy**

This policy has content dealing with IT disaster recovery, which is a vital component of ICPSR's disaster plan. The policy provides guidelines on disaster recovery planning, and the maintenance, testing, and training of the recovery plan.

**Florida State University: Information Technology Disaster Recovery and Data Backup Policy**

While the data backup portion is of limited use (ICPSR currently maintains a backup policy as part of its preservation mission), the recovery section is of interest. The policy has a definition of Best Practice Disaster Recovery Procedures, as well as an outline of the university's own IT recovery planning and implementation procedures. This section of the policy is guided by the "IT Contingency Plan" contained in NIST's Contingency Planning Guide for Information Technology Systems, which has guided much of ICPSR's disaster planning to date.
Designing a Disaster Planning Program

**Michigan State University Disaster Recovery Planning: Step by Step Guide**

This program breaks down the disaster planning process into steps, and provides information relevant to individual units within a university setting.

**Minnesota State Archives: Disaster Preparedness**

This document is a detailed guide to the disaster planning process. While mostly dealing with paper records, the document does a good job of identifying different roles and responsibilities for members of the planning and recovery team. This is the most complete listing of these roles out of all the resources listed here.

**Cisco Systems: Disaster Recovery Best Practices White Paper**

The paper outlines disaster recovery using the framework of the above resources, but tailors it to an IT point of view. It has useful information on how to prepare and recover both hardware and software assets.

**AT&T: Key Elements to an Effective Business Continuity Plan**

A short paper that summarizes business continuity planning in the private sector.

## Relevant Disaster Planning Programs

**OCLC Digital Archive Preservation Policy and Supporting Documentation**

This document has a clear articulation of OCLC’s disaster policy, along with outlining disaster prevention and recovery procedures and a time-frame for the restoration of services in the event of a disaster. The policy includes a good definition of a disaster prevention and recovery plan: “A set of responses based on sound principles and endorsed by senior management, which can be activated by trained staff with the goal of preventing or reducing the severity of the impact of disasters and incidents.” Interestingly, OCLC embeds its disaster plan within its overall preservation policy, stating: “The goal of disaster prevention is to safeguard the data (content and metadata) in the Digital Archive and to safeguard the Digital Archive’s software and systems. For disaster prevention and recovery, all data (content and metadata) is considered of equal value.”

### Staff Training

**dPlan.org**

This site provides useful information on training and an online form that would be useful in assigning trainers and monitoring the training process.

**CalPreservation.org: Disaster Plan Exercise**

This site offers roles and teaching points for a role-play training exercise that focuses on a disaster in a library.

### Examples and Tools for the Documentation Outlined by NIST Guide

The USDA has a full Disaster Recovery Plan, which outlines all of the documents outlined in the NIST Guide.

### Continuity of Operations Programs (COOP)

**FEMA: Continuity of Operations (COOP) Programs**

This site contains useful information on government policy, templates, and training resources to assist in the creation of COOP. Even though these are created for governmental agencies, they may be useful in guiding the COOP drafting process for others.

**Ready.gov: Ready Business Mentoring Guide, Working with Small Businesses to Prepare for Emergencies**

This site presents guidelines for composing a business COOP, including what outside actors should be involved in the planning process.
**The Florida Department of Health: Continuity of Operations Plan for Information Technology**
This is a checklist outlining key COOP tasks and responsibilities (see attachment E.7).

**Florida Atlantic University Libraries: Continuity of Operations Plan**
This document is a detailed working COOP, which includes reactions to specific disaster scenarios.

**Continuity of Support Plan/IT Contingency Plan**
See the USDA Disaster Recovery Plan for an example of a Continuity of Support Plan/IT Contingency Plan.

**Crisis Communications Plan**
Ready.gov: Crisis Communications Plan
This site suggests guidelines for composing a business disaster communication plan, and includes good suggestions for the plan’s Web presence.

North Carolina State University: Standard Operating Procedures for Crisis Communications
This is the policy and plan for the University as a whole. While much of this policy deals with communication at a high level, there are useful sections that may guide communication plans, such as whom to identify as vital contacts within the organization (including whom to contact first), and how to manage external communications. The Missouri S&T: Crisis Communication Plan is also a good example.

There are some disaster communication guidelines provided online by for-profit companies that offer crisis planning services. Two of these are FEI Behavioral Health: Crisis Management Disaster Communication Plan and LawBiz: Disaster Communication: Develop a Plan and Know How to Execute It.

**Disaster Recovery Plan (DRP)**
DevX.com: How to Create a Disaster Recovery Plan
This is an online article on planning and testing a DRP in a for-profit organization.

University of Arkansas: Computing Services Disaster Recovery Plan
This document provides a complete and thorough plan that outlines the initiation of emergency and recovery procedures, and addresses how the plan will be maintained.

Adams State College (CO): Information Technology Disaster Recovery Plan
This plan has a thorough section on risk assessment.

**Written Resources**
