

NUMBER

82

Preparing for the Worst: Managing Records Disasters

By
Ann Marie Przybyla
Geof Huth

2004



The University of the State of New York
The State Education Department
New York State Archives
Government Records Services
Albany, New York 12230
<http://www.archives.nysed.gov>

THE UNIVERSITY OF THE STATE OF NEW YORK
Regents of The University

ROBERT M. BENNETT, CHANCELLOR, B.A., M.S.	Tonawanda
ADELAIDE L. SANFORD, VICE CHANCELLOR, B.A., M.A., P.D.	Hollis
DIANE O'NEILL MCGIVERN, B.S.N., M.A., PH.D.	Staten Island
SAUL B. COHEN, B.A., M.A., PH.D.	New Rochelle
JAMES C. DAWSON, A.A., B.A., M.S., PH.D.	Peru
ROBERT M. JOHNSON, B.S., J.D.	Huntington
ANTHONY S. BOTTAR, B.A., J.D.	North Syracuse
MERRYL H. TISCH, B.A., M.A.	New York
GERALDINE D. CHAPEY, B.A., M.A., ED.D.	Belle Harbor
ARNOLD B. GARDNER, B.A., LL.B.	Buffalo
HARRY PHILLIPS, 3RD, B.A., M.S.F.S.	Hartsdale
JOSEPH E. BOWMAN, JR., B.A., M.L.S., M.A., M.ED., ED.D.	Albany
LORRAINE A. CORTÉS-VÁZQUEZ, B.A., M.P.A.	Bronx
JAMES R. TALLON, JR., B.A., M.A.	Binghamton
MILTON L. COFIELD, B.S., M.B.A., PH.D.	Rochester
JOHN BRADEMAS, B.A., PH.D.	New York

President of The University and Commissioner of Education

RICHARD P. MILLS

Chief of Staff

Counsel and Deputy Commissioner for Legal Affairs

KATHY A. AHEARN

Chief Operating Officer

Deputy Commissioner for the Office of Management Services

THERESA E. SAVO

Deputy Commissioner for Cultural Education

CAROLE F. HUXLEY

Assistant Commissioner for State Archives

CHRISTINE WARD

Chief, Government Records Services

ROBERT W. ARNOLD

.....
The State Education Department does not discriminate on the basis of age, color, religion, creed, disability, marital status, veteran status, national origin, race, gender, genetic predisposition or carrier status, or sexual orientation in its educational programs, services and activities. Portions of this publication can be made available in a variety of formats, including braille, large print or audio tape, upon request. Inquiries concerning this policy of nondiscrimination should be directed to the Department's Office for Diversity, Ethics, and Access, Room 530, Education Building, Albany, NY 12234.

Table of Contents

Introduction	1
First Steps in Developing a Disaster Management Plan	3
1. Preventing the Worst	5
2. Responding to a Records Disaster	14
3. Getting Back to Work	20
4. Keeping Your Disaster Management Plan Current	23
Online Sources of Information	24
For More Information and Assistance	24
Appendix A: Outline for a Disaster Management Plan	25
Appendix B: Data Collection Forms	27
Appendix C: Sample Disaster Management Plan	38
Appendix D: Glossary of Disaster Management Terms	50



Introduction

Disasters do happen

Many organizations assume they will never experience a disaster, so they never develop a strategy for preventing or responding to one. Even if they do have a formal disaster response plan, chances are it does not address the need to protect one of their most valuable assets: their records. The reality is that annually in New York State dozens of state agencies and local governments experience calamities—ranging from floods and fires to hard drive crashes—that affect their records and cost thousands of dollars in recovery.

You can significantly reduce the impact of a disaster in terms of property, business, and even human costs if you recognize that disasters do happen and if you actively work to anticipate and prevent them. A strong disaster management plan will help you avoid or manage events that can threaten, damage, or destroy your records. This publication provides guidance on developing a strategy for managing a records disaster and describes how to integrate that strategy into a larger, organization-wide disaster management plan and your ongoing records management program.

Why protect records?

Records consist of information recorded on paper, film, electronic, and other media that an organization creates and receives in the regular course of its official business. A *records disaster* is a sudden, unexpected event that significantly damages or destroys records or prevents access to the information they contain. A disaster differs from neglect, which involves ignoring a chronic problem that will lead to substantial information loss over time. A sudden flood that dampens records—creating the potential for mold infestation—is a disaster, whereas mold growth on records that have been stored for years in a wet basement is the result of neglect.

Most of the costs of disasters are immediate and obvious, but some are long-term costs that are difficult to calculate. A records disaster can deprive you of the information you need to resume normal

operations. In private industry, a loss of information can cause businesses to fail. In any organization, it can lead to staff frustration and decreased productivity, impair services to citizens, deprive you of evidence needed in court, and make it impossible to document your revenue and assets. By extension, it can cause citizens to lose confidence in your ability to do your job and protect their interests. In many ways, a records disaster can ultimately lead to a public relations nightmare.

For the purpose of this publication, *disaster management* encompasses three different activities:

- *Disaster mitigation*, the process of anticipating potential disasters by having in place a system of preventive measures
- *Disaster remediation*, work undertaken to lessen the impact of a disaster after it has already occurred
- *Business continuity*, measures that are necessary for the swift and efficient resumption of daily operations after an emergency

Managing records disasters effectively can

- guarantee a secure environment for ongoing records storage and maintenance
- ensure the physical safety of employees who regularly retrieve, use, and manage your organization's records
- identify and protect records vital to your operations
- identify and protect your archival records
- provide a framework for responding safely and efficiently to disasters when they do occur
- allow you to resume your work as soon as possible after a disaster

To manage records disasters, you must first develop a formal, written plan that specifically addresses those events that could potentially damage or destroy your records. A good disaster management plan will include strategies for

- preventing potential disasters by identifying and reducing risks
- responding directly to disasters if they do occur
- continuing normal business operations after an emergency has passed
- periodically reviewing and adapting your plan to reflect current conditions

Each of these four activities will be discussed in detail below.

First Steps in Developing a Disaster Management Plan

Getting support and cooperation

Because of the scope and impact of disaster management, your first step must be to convince management to support development of a plan. You may have to use various means of persuasion and types of evidence to convince management of the absolute need to add this responsibility to your workload. Demonstrate to your chief administrative officer or board how your organization's records are vulnerable by noting obvious risks and referring to previous mishaps and close calls. Cite the devastating impact of records disasters that have occurred in organizations similar to or located near your own. Give solid estimates of the costs your organization would face if it experienced a serious records-related disaster. For example, estimate the potential costs of having insufficient evidence for lawsuits, the costs of freeze-drying and fumigating damaged records, and the potential for loss of human life. Offer to write the disaster management plan or oversee its development, providing an outline or proposal on how you will proceed. Without management support it will be difficult—if not impossible—to prepare and implement an effective, comprehensive disaster management plan.

The plan also has a greater chance of success if developed as a cooperative project that involves staff from across your organization. Rely on your co-workers to provide the background information (the records they create, their job functions, and work environment) that is essential to an effective plan. Staff must be committed enough to the plan to implement it as needed and to ensure that it remains a current, living document. To gain staff cooperation, circulate a memo of support for the project from management and notify everyone of the phases of the plan's development, especially its ultimate completion.

Deciding who will write the plan and how

You will need to decide who will be responsible for writing your organization's disaster management plan. If you don't have the time or expertise, or if you prefer to use an objective outside expert, hire a consultant to prepare the plan for you. If you choose to work with a consultant, prepare a detailed contract so that the person you hire knows and legally acknowledges your expectations for the project. Form an in-house review committee to assist the consultant, read through drafts of the plan, and request revisions as necessary. Schedule enough time for the consultant to interview all department heads and key staff, assess your facility's risks, and conduct research,

so that the finished plan is not a generic document but is specifically tailored to your organization and its needs. Ensure that the consultant knows exactly what you want your disaster plan to cover. Some plans will focus only on records disasters; others will address any disasters affecting your organization's facilities or any civil disasters within its borders.

You can also write the plan in house. If you do, first form a planning team that includes your records manager and, if possible, staff from information technology, facilities maintenance, finance, planning and development, and others. The disaster management planning team will be responsible for gathering information, inspecting current sites and adjacent conditions, conducting background research, and reviewing various drafts of the plan. You can even ask team members to prepare the sections of the plan that directly relate to their work responsibilities. Set an agenda and develop a reasonable timeline to ensure that the project continues to move forward in spite of your respective workloads.

If you prepare the disaster plan in house, use the resources in the appendices to guide its development. You can adapt these tools to suit your own organization's needs, adding or deleting sections as necessary. Appendix A, "Outline for a Disaster Management Plan," sketches out the main elements and basic organization of a disaster management plan. Appendix B, "Data Collection Forms," includes a number of forms designed to help you plan for and respond to records disasters. Appendix C, "Sample Disaster Management Plan," provides a model you can use as the basis for your own plan.

Your team could purchase disaster planning software from vendors that specialize in marketing disaster management products and services. Disaster management or business continuity planning software features interactive templates and assessment forms that your team can fill in with information specific to your organization. The software helps you identify your particular risks, choose possible ways to reduce those risks, design a disaster plan, and determine how to respond to different types of disasters. Such software does not write a disaster plan for you but will help guide you through the process and remind you of risks and solutions you may not have considered.

The State Archives is also available as a resource for providing direct technical assistance and advice on how to prepare a disaster management plan. Funding for disaster recovery planning, including money to hire a consultant and purchase planning software, is available to local governments through the Local Government Records Management Improvement Fund (LGRMIF), as are grants to support many of the facility enhancements necessary to protect your

records. Local governments can also apply for emergency funding to pay for disaster recovery efforts related to records. For further information about any of these services and grants, contact your State Archives regional advisory officer (RAO), or Government Records Services in Albany at (518) 474-6926.

1. Preventing the Worst

Identifying the irreplaceable: Vital and archival records

Risks are especially acute when they threaten your most valuable resources. When writing a disaster management plan for your records, first identify those that merit the most protection, identify and evaluate serious threats, and devise measures to reduce or eliminate those risks.

Your organization's most valuable records are its vital and archival records. *Vital records* are those records that, if destroyed, must be recreated to resume essential business functions. They provide evidence of your organization's assets and the rights of your customers. Records that are vital are different from those that are merely important; without vital records, you and your organization cannot function. In disaster management, the term "vital records" does not refer to birth, death, and marriage records, which municipal clerks in New York call either vital records or vital statistics. Vital records tend to be active, documenting the status of ongoing, current transactions and relationships. Increasingly, vital records are created and accessed electronically. Some examples of vital records are

- tax bills and receipts for the current year
- property records
- open contracts
- active case files
- records of unfinished construction projects
- payroll records

You can identify your vital records by conducting a comprehensive records inventory or by undertaking a more focused survey where you ask staff to identify those records they absolutely need to do their job. You must also determine which functions are critical to your organization. Those records that are essential to support the critical functions of your organization are your vital records. Typically, only five to ten percent of all records an organization creates are vital.

Archival records are those that have enduring historical value. In New York State, archival records are any government records that have been identified as permanent in a State Archives disposition schedule or simply any other records that you have determined to be historically significant. Archival records can be—but usually are not—vital records. Some examples of archival records are

- annual reports
- tax assessment rolls
- board minutes

As with vital records, you can identify archival records by conducting either a comprehensive inventory or a focused survey. Few records that you create actually have archival value.

Identifying risks through analysis and probability

Once you have identified and located your vital and archival records, determine possible threats to their safety and integrity. Risks to your records come in many forms. You are probably aware of several obvious ones, but to develop a good disaster preparedness strategy you must systematically identify, analyze, and prioritize all risks. First, identify existing risks inherent in your organization's location and operating procedures. Then identify disasters that are likely to occur simply because they have happened repeatedly in the past. Consult newspapers and records such as minutes, capital project files, and financial records to determine how often you have had the same type of disaster and what the average cost of recovery has been. Be aware of the potential impact of current events as well. Consider whether the role of your organization or the general political environment could make you a target for vandalism. Determine whether your organization is vulnerable to acts of terrorism, especially if it is near a major metropolitan area or important resources such as a water supply, utilities, or transportation lines. Your research and analysis will give you a working list of probable risks.

Identifying human threats

Humans are the single most common cause of disasters affecting your records. It's therefore important to factor into your analysis the role of your staff and members of the public when identifying and addressing risks. While vandalism, arson, sabotage, and terrorism are extreme examples of what people can do, more often staff members accidentally delete files, neglect to create appropriate backups of their work, fail to destroy obsolete records, cause unintended damage during construction projects, and generally mishandle or lose

important records. Human threats are sometimes intentional (as with computer hacking) and sometimes accidental (staff unknowingly overwriting important files when installing software). Although common, human threats are the hardest to control and impossible to eliminate. You can, however, implement strategies to protect your records from human risks, once you recognize the types of damage they can cause.

Identifying risks to electronic records

Information is increasingly created, accessed, and stored electronically. Several characteristics of electronic records make them vulnerable in ways that paper records are not. Electronic records are stored on media and devices—magnetic tape, CDs, DVDs, detachable hard drives, computers, and servers—that are relatively easy to carry and conceal, so people are more likely to misplace or steal them. At the same time, electronic storage media can hold a large volume of records in a very small physical space. As a result, you can suffer a crippling loss of information if they are damaged, particularly if you don't have secure backups. Also, electronic media are easy to erase, either accidentally or intentionally.

If not properly protected, electronic records are also susceptible to unauthorized access. While staff may accept the concept of storing important or confidential papers in locked file cabinets and storage vaults, they may be less sensitive to safeguarding the same information on personal computers (PCs) and storage media in busy office areas. Because of the prevalence of PCs, individual employees have unprecedented access to information across an organization, especially if they work on shared drives of a local area network. If you have access to the Internet, you are vulnerable to vandalism from hackers or destruction from viruses. It is important to know the risks associated with your electronic records because salvaging them after a disaster can be very expensive and can require the services of a specialized vendor.

Identifying risks through site assessment

The best way to identify existing risks to your records is to conduct a comprehensive site assessment, using the “Risk Identification Checklist” form in Appendix B. Assess your site in consultation with building custodians, engineers, architects, and anyone familiar with the details of your organization's facility and its environment. Below are some elements to consider during the assessment.

Natural environment

Consider the geography, climate, and other natural conditions where your organization exists. For example, are you located in an area that characteristically experiences severe weather patterns such as electrical storms, tornadoes, hurricanes, and snow and ice storms? Are you near a heavily wooded area prone to forest fires in hot, dry weather? Are your facilities located on a fifty- or 100-year flood plain? Are you near or on a fault line? Although relatively rare in New York, earthquakes do occur, causing cracks in foundations, misalignments in sewage and electrical systems, and other structural damage. These natural disasters make recorded information susceptible to damage or loss from water, fire, sewage, and electrical disruptions.

Built environment

Assess your immediate surroundings, especially in terms of your organization's proximity to sources of potential problems. Are you near a railroad track or highway where hazardous materials are shipped? Do chemical or nuclear industries operate nearby? Are large trees and telephone poles located too close to your facility for safety? Is a large construction project beginning near or on your property? Is your facility located near a site frequently used for large public functions, such as parades, neighborhood festivals, or political demonstrations? Is your building itself used for other public purposes? In other words, are your records vulnerable because of conditions that disrupt standard operating procedures and allow outsiders access to your facility?

Building structure

Analyze the various facets of any buildings where you and your co-workers create, store, and access records. Evaluate the roofs, walls, windows, foundations, and other structural elements. Are they strong and impermeable, or weak and prone to leakage? Inside, check the quality of electrical wiring, sewer lines, and water and steam pipes. Are critical repairs or upgrades needed? Are they included on a periodic maintenance schedule? Determine whether a basement used for records storage tends to flood and, if so, how often and under what conditions. If your storage room is on an upper floor, consult with an engineer to determine whether the floor can support 300 pounds per square foot, the recommended weight-bearing capacity for records storage. Consider the materials used to construct your facility. Do you work in a newer building with walls that can't support shelving loaded with records? Are you in an older, predominately wooden structure? Does your building have adequate fireproofing and a fire suppression system? Also be aware that the same sprinkler systems and fire extinguishers that can save your property from complete destruction can cause serious damage to records.

Storage conditions

Serious disasters can occur in the very places where records are stored. Are your inactive storage areas clean, well lit, dry, and free of mold? Are your records stored in sturdy, standard cubic-foot boxes on steel shelving of an appropriate strength? Is the bottom shelf at least four to six inches from the floor so that records stay dry during minor flooding? If you store records in a basement, are your vital and archival records on an upper shelf (safer in case of floods) but not under pipes of any kind? Do you regularly purge obsolete records? If you don't, you probably have an unnecessarily cramped and crowded storage room, which can create unsafe conditions for both your staff and the records. Do you have reliable backups for your electronic records stored offsite?

If you need guidance on assessing and enhancing your storage areas, contact your RAO. The State Archives also provides written guidelines for setting up inactive records storage areas, specifications for shelving appropriate for records storage, and lists of shelving and other vendors.

Estimating costs

Determine the potential costs of disasters to convince management of the need for a plan, compare the costs of recovery to those of initiating preventive measures, and budget ahead to respond to the likeliest disasters. You can also prioritize potential risks by estimating the relative costs of different types of disasters. Estimating possible recovery costs is never an exact science, but several methods do allow you to be fairly precise.

Base your estimates on the projected cost of losing specific records series or access to them. For example, calculate the labor hours needed to rekey data into an electronic records system, the cost of recovering essential data, the potential loss of income that would result from the unwanted destruction of vital records series, and the cost of litigation for which you lacked sufficient evidence. You can also use the following formula to estimate your *annualized loss expectancy*, or the amount that you could lose annually if a specific kind of disaster occurred:

$$\text{Probability (P) x Cost (C) = Risk (R) or potential loss}$$

In this formula, P represents the probability that a threat will occur in any given year. If a specific kind of disaster is likely to occur once a year, P equals 1; every two months, P = 6; every four years, P = 0.25; every ten years, P=0.10, and so on. Provide costs, or C, in terms of the

dollar amount of replacing, reproducing, or doing without a records series. For example, if you know that a flood tends to occur every ten years, and the potential cost of litigation for which you didn't have the necessary records is \$25,000, then your annualized loss expectancy or risk is \$2500. This formula is a useful way to develop consistent figures on the potential costs of records disasters, which you can then compare to those of prevention.

Insurance coverage

Insurance is an important element of disaster management. The kind of insurance coverage you have will be a factor in determining the cost of planning for and recovering from a disaster. When selecting insurance, your organization has one of three choices. First, you could choose not be insured at all, which is unlikely and inadvisable. Second, you could be self-insured, which means that your organization annually sets aside a sum of money to cover losses that could occur as the result of a disaster. Base the amount of your self-insurance fund on a thorough analysis of all risks and their associated costs, so that you have enough money to fully recover from any disaster. In choosing to be self-insured, your organization assumes that the cost of paying for disaster recovery will be less than paying premiums over an extended period of time.

Third, and most likely, your organization could have insurance through an outside provider. If so, you must know and understand the terms of your policy. Ideally, your insurance will allow for the replacement or restoration of records. Determine whether you have actual cash value or average cost value to replace damaged or destroyed equipment and other property. Verify whether you have an all-risk policy or one that covers "acts of God" only partially or not at all. Determine if you need special insurance coverage, such as flood insurance. Generally, the more expensive your insurance, the more it will cover.

To help develop the response section of your plan, determine what you are expected to do in the event of a disaster to meet insurance requirements. For example, determine whether an insurance agent must personally inspect the disaster site before you begin recovery efforts, or whether your carrier requires photographs to document damage. Once you understand your insurance coverage, you might recommend that your organization either acquire insurance coverage, increase the level of self-insurance, or upgrade an existing policy. Include a description of your insurance coverage in your disaster management plan and incorporate details of coverage into the response section of the plan.

Preventive and protective measures

After you have finished gathering data on all risks, your disaster management team is ready to start developing strategies to help prevent disasters from happening. You may find you can fix some minor problems immediately, even in the data-gathering stage. For example, if you discover during your site assessment that your oldest minutes book rests beneath a steam pipe in a basement storage area, move the volume to a safer place—either above ground or to a less vulnerable shelf—as soon as possible.

The single most important step you can take to protect your records is to establish firm control over them. If you haven't already done so, conduct a comprehensive, detailed records inventory or establish a database locator system that identifies your vital and archival records and that helps you to systematically dispose of obsolete and non-record materials. Establish written procedures for the various facets of your records management program, including creation, retention, storage, and access. An organized records management program is the best line of defense for protecting your records.

You can also address many serious risks to your records by establishing preventive measures in your facilities maintenance schedule. Below are two scenarios that a risk inventory might reveal, followed by lists of some appropriate protective measures:

An analysis of local newspapers, records books, and popular lore indicates that you live in an area that experiences a major ice storm about every three to five years. The ice storms frequently cause secondary disasters such as downed trees and power lines, electrical fires, burst pipes, and computer crashes.

Possible responses:

- Install an emergency generator that keeps necessary electrical systems operating at a minimal level during power outages.
- Set a schedule for periodically inspecting and servicing your emergency generator.
- Make sure your computer equipment has power-surge protection.
- Back up electronic records more frequently during months when ice storms are more likely to occur.
- Regularly trim back tree branches that would otherwise grow over your building.
- Set a schedule for inspecting your electrical and plumbing systems.

Your inactive records storage room has appropriate steel shelving, good lighting, and records boxed and fully labeled in standard storage cartons. Upon investigation, however, you find that it shares a wall with a custodian's closet that contains cleaning solvents, paint thinner, and other flammable materials.

Possible responses:

- Store the custodian's work materials in a new area, preferably a storage shed or garage outside of the building entirely.
- If no other space is available, be sure that the inactive records storage room is protected either with cement block walls or an appropriate grade of fire-resistant sheetrock.
- Install a good fire alarm and suppression system.
- Set an annual schedule for inspecting and testing the fire alarm and suppression system.

Your custodial and facilities management personnel will know the precautions that are already followed and resources that are on hand to maintain your site. The disaster management team needs to work with them to ensure that they have accounted for the safety and security of records in their existing maintenance schedules.

Protecting electronic records

To protect your electronic records effectively, ensure that written policies and procedures regulate their creation, maintenance, and daily use. Some basic steps to ensure the security of your electronic information include the following:

- Encourage staff to use passwords and to change them frequently to protect information on their PCs. If staff resist these measures, program your system to enforce the creation and regular changing of passwords.
- Use firewalls and anti-virus software to protect electronic information on a network. Maintain a schedule to ensure that you regularly upgrade your system's security features.
- Create backups of your electronic records at appropriate intervals. Store the backups offsite in a location sufficiently distant from where you create and maintain the original records. For instance, make sure your backups are out of reach of a forest fire or flood that could affect your primary site.
- Provide ongoing technical training for staff who are directly responsible for creating and using electronic records

Also consider establishing alternate sites where you can access and use your electronic records, especially those that are vital to your business operations. Alternate sites can have varying levels of functionality, depending on the importance of your electronic records and what your budget will allow. A *cold site* is an available, empty space where you can move your own computer equipment and data after a disaster has deprived you of your usual workplace. A *warm site* contains some of the equipment and data you need and allows you to conduct your work at a reduced capacity. A *hot site* completely mirrors your primary facility, duplicating all computer equipment and data. You can establish these sites either through a reciprocal agreement with a neighboring organization or by contracting for space through a commercial vendor.

When prevention isn't enough

Although you can minimize the probability and severity of disasters, you can never completely prevent them. There will always be conditions such as severe storms and other natural disasters that are beyond your control; no matter how much you prepare for them, they will occur at regular intervals and have some impact on your organization. On the other hand, prevention might exceed the potential costs of recovery, especially if it involves an expensive purchase, construction project, or upgrade. Because of lack of time or money, you will probably not be able to address every identified risk, and certainly not right away. Your goal is to mitigate your risks as much as you reasonably can, given your means and the cost of potential disasters.

For these reasons, you will need to develop an appropriate disaster response plan beforehand. For example, if your organization faces the two risks outlined in the previous section, develop plans for responding to ice storms and fires or explosions. A significant part of your disaster management plan is a set of individual response plans for specific types of disasters.

2. Responding to a Records Disaster

Staff training

Your disaster response plan will essentially be useless if your staff do not know of its existence and are not properly prepared to implement it. For this reason, involve staff in the response planning process. Determine where they are most likely to be if a disaster happens both during and after work hours. Identify who is responsible for the care of vital records, archival records, information technology, and building operations. Since most disasters occur after normal working hours, include night staff such as security or custodial personnel in your training program. Give key members of your organization prominent roles in an actual disaster response, as described in the next section.

After management has given final approval, distribute your plan to all staff. Always provide copies of the plan to new staff members as part of their orientation. Even after extensive training, if people do not have access to the plan and are not familiar with its contents, any disaster response will be significantly compromised.

Test your response plan to make sure it is feasible, and help familiarize staff with their roles and responsibilities. First implement tabletop testing, which involves having your staff read through the plan together around a table, following the steps in each response to make sure that the sequence of actions and assigned responsibilities makes sense. You can also conduct occasional simulation drills where staff practice responding to a disaster. Test any alternate sites that you've designated for your electronic records, make sure your backup system works, and verify that backup tapes can be reloaded and used. These drills are useful not only for testing various elements of the plan but also for training staff.

Working with local emergency personnel

Good disaster planning will involve local emergency personnel. Meet with fire response units in your community, provide them with floor plans of your buildings, and give them a tour of your facilities. Explain your needs and solicit ideas on how to improve the safety of your buildings and protect your records. Emergency personnel will then be more familiar with your facilities and better able to protect your interests, especially if they are the first on the scene. Additionally, consider staging cooperative drills with emergency units to assess response times and work out any unexpected logistical problems.

Preparing an effective response

The goal of planning a disaster response is to ensure the safety of your organization's records under stressful circumstances and to allow the swift resumption of normal business operations. Your plan needs to provide a list of resources for employees to consult in the event of any kind of records disaster. Use the "Disaster Response Checklist" in Appendix B to gather information about those resources.

Members of your response team

You will need a response team to implement your response plan effectively. A good team consists of key staff from across your organization. Designate a team leader as well as an alternate in case the leader can't be reached quickly in an emergency. Also include on the team the person in your organization who is directly responsible for your records, such as the records management officer (RMO) in a local government or state agency. Other valuable team members include a building custodian, a financial officer, the person in charge of your electronic systems, and one person to act as a liaison between your organization and the media. If you plan to use volunteers for salvage efforts, indicate in your plan who will mobilize, coordinate, and oversee your volunteer staff. Also designate someone to document the impact of the disaster and your recovery efforts. You will need such documentation to satisfy insurance requirements, provide information to the public, and assess the effectiveness of your disaster management program in general and the response in particular.

Phone tree for the response team

A phone tree is a way to distribute responsibility for notifying the response team. Whoever first discovers the disaster must know to call the response team leader or alternate. Then the leader or alternate calls two or three team members, who in turn will contact members further down the phone tree, and so on, until the entire team has been alerted.

Emergency telephone numbers

Include contact information for resources outside of your organization. Provide numbers for local police and fire agencies, utility companies, your insurance agent, county and state health departments, the State Emergency Management Organization (SEMO), and the Federal Emergency Management Administration (FEMA). Consider vendors and other service providers who specialize in responding to specific types of emergencies. For example, when planning a response for floods, fires, chemical spills, and computer crashes, include contact information for vendors who provide freeze-drying and fumigation services, hazardous materials (hazmat) teams, and data recovery

specialists. Be sure to include the name, telephone number, and e-mail address of your State Archives RAO as well as the State Archives' general telephone number in Albany.

Salvage priorities

Many plans include a short records inventory with the name, volume, and location of an organization's vital and archival records, including those stored electronically. You can include a floor plan that shows the location of your most important records series, whether kept in office or storage areas. To make these records easier to find in the event of an emergency, attach colorful or glow-in-the-dark labels to pertinent filing cabinets and records storage containers.

Disaster response supplies and equipment

Have a small number of general-purpose supplies available at all times, including extra records storage boxes, industrial fans, rubber gloves, plastic sheeting, and a portable sump pump. Be aware, however, that some disasters demand more resources for response and recovery than you could reasonably expect to have on hand. Maintain a current equipment inventory that indicates the location of fire extinguishers and hoses, turn-off valves for gas and water, and electrical system and alarm shut-off switches.

Floor plans and area maps

Supplement narrative information with floor plans that indicate salvage priorities, important supplies, and internal controls for information, electrical, and plumbing systems. Use maps or a geographic information system (GIS) to record information useful for disaster recovery, including onsite and adjacent risks, as well as important resources such as water mains, emergency routes, and hydrant and equipment locations.

Steps of an effective disaster response

Each disaster response plan must include a series of steps for staff to follow, beginning with the initial discovery that something is wrong. Indicate in the plan who in your organization has responsibility for each step. The purpose of these instructions is to provide an orderly frame of reference in a chaotic situation. Be especially sure your staff understands that human safety is the primary objective during any disaster response. Dedicated employees may feel obligated to take unnecessary risks to rescue records and other property, but they must understand that nothing is worth injury or loss of life. Your goal—and that of your response plan—is to prevent complete chaos, which could lead to secondary disasters, personal injury, and a greater impact of the initial disaster.

Below are the basic steps to include in every disaster response plan:

a. Identify an emergency

This is the one part of your disaster response that you can't plan. A disaster can happen at any time and be discovered by anyone.

b. Notify the team and others

Whoever discovers the emergency must contact the team leader or alternate. The team will then implement the phone tree.

c. Assess the situation

Estimate the amount of time that has elapsed since the disaster occurred, assess the level of impact during that time, and attempt to project how quickly the situation will deteriorate. Check the current temperature, humidity, and air circulation. Look for damaged pipes of any kind and standing water or other fluids. Also check for downed branches and power lines or submerged electrical wires. Make sure there isn't so much particulate matter in the air from burnt building materials or chemicals that it poses a threat to the response team.

d. Identify the appropriate response

The team must work together to identify an appropriate initial response. Although every disaster is different, the team should follow responses already outlined in your response plan. For example, if an ice storm has brought down trees and power lines, your plan might recommend that the team contact the electric company and summon custodial staff to help remove downed branches. The plan must contain contact information for the utility company and indicate locations of chainsaws and other useful equipment. The team must continue to assess, reassess, and respond as the disaster and recovery efforts unfold.

e. Stabilize the environment

Don't enter your facility or affected area until it's safe to do so. In many cases, you will have to rely on others to stabilize the situation first, especially in cases of fire, severe floods, downed trees or power lines, or damaged roofs or exterior walls. If there is standing water in any location, be sure to turn off all electric power before entering the area.

Once it's safe to enter, try to stabilize the temperature at about 65 degrees and the humidity between 45 and 55 percent. If an area is flooded or has high levels of humidity, reduce the temperature further to delay the onset of mold infestation, keeping in mind that mold can grow within forty-eight hours. Remove standing water as soon as possible.

f. Identify new or continuing threats

Many disasters can trigger a secondary threat. Check for leaks of any kind, including natural gas, steam, sewage, and water. Try to determine whether the potential exists for contamination from chemicals, asbestos, or mold. Assess the building's exterior, foundations, support beams, and supporting walls for structural damage. The response team must determine how to act if the risks increase.

g. Take photographs

Photographs are useful for measuring damage and formulating methods of response and recovery. They may also be necessary to satisfy the requirements of your insurance.

h. Assess damage

Use the "Initial Damage Assessment Inventory Form" in Appendix B to gather preliminary data about the disaster's impact on your records. Assess the severity of damage, from minor impact to total destruction. Estimate the total quantity of records affected, and identify the name, quantity, and format of each records series involved.

i. Develop salvage strategy

Salvage is essentially a process of triage. If some affected records have already met their legal retention periods, tag them for destruction rather than attempt to move them to temporary storage. Of the remaining records, identify those you need to retain temporarily and those that are permanent. If the records are not vital or permanent, set them aside to consider the resources you can expend on repairing them or preventing further damage. If any of the remaining records are vital or archival, take steps necessary to make them usable, as described below.

j. Implement salvage strategy

Start moving the records from the affected area to temporary storage. Be sure to consider staff involved in salvage efforts. For example, if the records are wet or fire-damaged, provide staff with rubber gloves and face masks. If air quality is especially poor, seek advice from your county health department on what protective clothing and breathing apparatus to use. Remember that disasters can be a source of stress, especially if they result in injury, death, or total destruction. Instruct all staff involved in salvage operations to work in short, rotating shifts. Arrange for food, water, and even grief counseling, if necessary.

On a frigid February afternoon, a water pipe burst in a county municipal center. Water descending from the pipe collected in the basement where the county stored its records, pouring onto shelves from above and reaching a depth of four to five feet. Approximately 1,200 storage cartons of records were either completely submerged or floating in muddy water.

Using information from an inventory he had completed the previous year, the county records manager determined that the submerged records included

- permanent court case records in the custody of the county clerk
- correspondence of the county manager and assistant county manager that might contain permanent records but consisted mostly of routine correspondence or records duplicated elsewhere
- patient files and X-rays (from a former county tuberculosis hospital) that had met the legal retention period but were historically significant
- purchasing files, including files pertaining to capital construction, current contracts, and closed projects
- social services cases that had not yet met their legal retention requirement
- permanent coroners' investigation case files

While a disaster recovery company removed the standing water, the county records manager arranged to move all water-damaged records that were clearly permanent to a commercial food-storage freezer. Afterwards, he worked with staff in the purchasing department to identify those portions of the damaged purchasing files related to capital construction and current projects. He transferred the capital construction files to the commercial freezer. Because the volume of current purchasing records was small, he air-dried them under industrial fans set up in the alternate storage area.

Given the expense of freeze-drying wet records, the county records manager decided to retain only a sample of the tuberculosis patient files and none of the X-rays. He requested and received permission from the State Archives for early disposition of the correspondence, social services food stamp distribution files, and non-permanent purchasing files documenting closed transactions.

At the end of this process of records triage, the county records manager had identified 100 cubic feet of permanent records to send to a freeze-drying vendor, including court case records and coroners' case files. He arranged to pay for the cost of freeze-drying with funds from a State Archives disaster recovery grant.

3. Getting Back to Work

Beginning the process of recovery

In addition to saving time and money, you can win a psychological victory for yourself, your staff, and your constituents if you get back to work as quickly as possible after a disaster. Your disaster recovery plan must include pre-determined locations where you and your staff can continue working if you lose access to your facility while it is being repaired or rebuilt. If the damage is minor, rearrange your remaining available workspace to accommodate displaced staff. If damage is extensive or complete, move to a pre-arranged hot or cold site, or at least try to continue essential operations in a neighboring business or government. Business continuity requires that you set up shop as soon as possible after a disaster, so you need a plan that details how you will resume your work: where you will locate temporary offices, what office equipment you will use, and what records and data you will have available to do your work. A detailed business continuity plan will also outline how long certain services can remain unavailable without causing irreparable damage to your work operations or public relations.

The cost of remediation and recovery

Contact your insurance agent to verify what your policy covers and then begin the claims process. Insurance will often cover the cost of cleaning or replacing damaged equipment, as well as repairing damage to records. If you work for a local government, contact the State Archives to determine if your government is eligible for a disaster recovery grant from the LGRMIF. If it is, work with your RAO to identify costs that are eligible for grant funding and to prepare a grant application.

At the same time, contact vendors who can remedy damage to your records. If you have lost a significant amount of vital data, contact a data recovery vendor or estimate the cost of rekeying data from available paper records. If you have a large number of wet paper records, hire a freeze-drying specialist to dry them completely. Follow the instructions outlined below for dealing with small numbers of wet records and for drying storage areas. Contact microfilm vendors to film smoke- or water-damaged paper records. After a flood or fire, you may need to call a fumigator to remove lingering odors and mold. Get estimates from contractors for the cost of repairing or rebuilding your physical facility.

To some extent, your recovery strategy will depend on associated costs, funding available from outside sources, and what you can afford. If the value of the records does not merit the cost of hiring a professional conservator or freeze-drying specialist, consider microfilming the records instead. If you have smoke-damaged records that you must retain for only a short period, store them in an isolated area until they can be destroyed rather than pay to clean and deodorize them. Determine whether rekeying data from existing paper records is feasible and cheaper than hiring a data-recovery vendor.

Wet paper records

Wet records are of critical concern because they can begin to grow mold within forty-eight hours. First, salvage any records threatened with further damage because they are under water or about to fall. Immediately reduce temperature and humidity levels in wet or humid storage areas, and set up fans, air conditioners, and dehumidifiers to help dry out these areas. If some boxes holding records are falling apart, temporarily store their contents in plastic crates to keep them neat and under control. You can use cardboard boxes if you don't have any plastic containers. After reboxing the records, move them to a safe and environmentally stable area. Finally, move all reboxed records to a dry, sheltered location. Never leave wet records to dry on their own, and do not leave them in an area with standing water, high humidity levels, or mold growth.

To remedy damage to the records themselves, move them to a cold, dry environment. If a large quantity of records is involved, check with local school districts, supermarkets, or businesses to see whether space is available in an industrial-size freezer for temporary storage. Then contact a vendor that specializes in freeze-drying records to extract moisture completely. If you are dealing with a small quantity of records, sort them according to type of material and dry them using the appropriate method listed below:

Damp, coated or uncoated paper: Fan pages open, insert blotter paper, and position them under a fan so air circulates between the leaves.

Wet, uncoated paper: Interleave pages with a paper towel or blank newsprint until damp, then remove the interleaving and proceed as above.

Wet, coated paper: Interleave pages with waxed paper, then fan open, and proceed as for wet uncoated paper.

Photographs: Rinse in clear, cold water. Dry them face-up on a blotter or hang them on a laundry line.

Once dried, place the records in new cartons. Label the boxes with records series titles, dates, and retention periods so that you know what each box contains.

Turning a negative into a positive

Although often devastating, disasters are an opportunity to improve your records management program, facility, staff assignments, and business operations in general. When recovering from a disaster, it is important not to replicate the same conditions that led to its occurrence. For example, if you are recovering from a flood, don't move records back into an area that has been dried and fumigated but that has the same dangerous conditions that caused the flood in the first place. Analyze all of the factors that caused the initial problem, and try to eliminate them. Some improvements to consider include the following:

- Impose strict environmental controls, conduct a comprehensive records inventory, develop a records locator system, and purge all obsolete records.
- Install steel shelving with bottom shelves that are four to six inches from the floor.
- Purchase lateral shelving and implement a color-coded filing system for active files, or, at the very least, evaluate pre-disaster filing systems to identify and remedy weaknesses.
- Install new or improved preventive measures, such as fire suppression, alarms, or electronic security systems.
- Develop policies and procedures that will enhance security. For example, if you have experienced an electronic systems crash that caused a significant loss of data, consider implementing a schedule of more frequent backups.
- Increase training for staff on records security, maintenance, and disaster management.

At some point, you will find that you have all of the elements necessary for full recovery and complete business continuity: a repaired or new facility, usable records, and staff ready to resume their normal work. Move dry, reboxed, relabeled paper records into inactive storage, noting changes in location in your database tracking system. Transfer current files back to work areas, and reload backup data. Move staff from alternate sites or work areas back to their own office space.

Then get back to work.

4. Keeping Your Disaster Management Plan Current

As with all policies and procedures, your disaster management plan is a living document that you must continue to review, evaluate, and adjust as needed. Develop a chapter that outlines the procedures your organization will follow to review and update the plan. In that chapter, specify which employees will do this and what their roles will be in the review process. Also include a schedule indicating how often you will review the plan. The review can take place at regular intervals, such as annually, or may occur when you change how you create and store information. For example, update your plan if your organization acquires a new information system or experiences significant staff turnover. At the very least, evaluate your disaster management plan every time you use it, analyzing to what extent the plan worked in practice and responding to any perceived weaknesses in your strategies. Indicate at the front of the plan when it was last reviewed and the period of time that it covers.

Elements of your review must include

- personnel contact information
- hardware and software information, including any changes to virus detection software and other security measures needed to protect data
- number and quality of resources necessary for business continuity
- new or increased threats that could require additional protection for your records
- alternate site requirements (for example, if you've recently automated a vital records series, consider upgrading from a cold site to a hot site or increasing the frequency of system backups)

As a final safety measure, maintain copies of your disaster management plan in offsite locations, including the homes of members of your disaster response team. Otherwise, if you keep all your copies in your offices, you may not be able to retrieve them during a disaster.

Online Sources of Information

Several online sources contain information on both disaster management planning and recovery:

Federal Emergency Management Administration (FEMA)

Provides recovery grants to those in federal disaster areas
www.fema.gov

State Emergency Management Office (SEMO)

Provides disaster management guidance and training, and financial assistance for disaster recovery
www.nysemo.state.ny.us

Northeast Document Conservation Center

Provides online disaster management publications and vendor lists
www.nedcc.org

Disaster Recovery Journal

Provides an online list of consultants, sources of disaster planning software, sample disaster management plans, training, and a free journal subscription
www.drj.com

For More Information and Assistance

The State Archives provides direct advice to state agencies and local governments on preparing for and responding to records disasters. The Archives also offers workshops on disaster planning and response. The Archives has regional offices throughout the state, and each office has an expert records specialist who can visit you and provide technical advice and assistance, especially in the case of a records disaster. The Archives can provide grants to local governments that have suffered damage to vital or archival records because of a disaster. The Archives' services also include publications and workshops on a wide variety of records management topics. For further information, contact either your regional office or

Government Records Services

New York State Archives

State Education Department
9A47 Cultural Education Center
Albany, New York 12230
(518) 474-6926
www.archives.nysed.gov

Appendix A

Outline for a Disaster Management Plan

This is a sample outline to help you prepare your own disaster management plan. Your organization may not require all of the elements listed below, or you may add to this outline as needed.

A. Policy and Planning

1. Introduction
Brief rationale for a disaster management plan
2. Glossary of Terms
Technical definitions for disaster and records management terms that appear in the text
3. Disaster Management Policy
Organizational policies relating to the development and maintenance of a disaster plan
4. Roles and Responsibilities
A list of staff and their specific responsibilities for disaster planning

B. Prevention

1. Introduction
Brief rationale for the need to mitigate risks and prevent disasters
2. Roles and Responsibilities
A list of staff and their specific responsibilities for preventing disasters
3. Site Maintenance and Inspection
Schedules and checklists to keep your physical facilities in good working order

C. Response

1. Introduction
Brief explanation of what disaster response entails
2. Roles and Responsibilities
List of staff and their specific responsibilities for responding to disasters
3. Actions in Case of a Disaster
Outlines of actions to take in response to specific disaster scenarios
4. Response Checklist
A checklist to help you determine which individuals to contact, how to contact them, and their initial assignments in a disaster. A complete checklist will include an emergency response phone tree.
5. Emergency Contact Telephone Numbers
A list of emergency contact telephone numbers: emergency response team, local police and fire departments, emergency response vendors, utility companies, hospitals, ambulance companies, the county health department, and the State Archives

-
6. Emergency Equipment Inventory
A list indicating the availability and location (onsite or offsite) of supplies and equipment that support disaster response, including fire extinguishers, smoke alarms, and shut-off valves
 7. Records Salvage Priority List
A list that details the locations of the archival and vital records to rescue in the event of a disaster
 8. Initial Damage Assessment Form
A blank copy of the form that will help your organization gather preliminary information about the extent of a disaster
 9. Floor Plans and Area Maps
Detailed floor plans of all buildings maintained by the organization (along with information on the location of records) and area maps that indicate the locations of important resources such as water mains and hydrants

D. Recovery and Business Continuity

1. Introduction
Brief explanation of what disaster recovery entails
2. Roles and Responsibilities
List of staff and their specific responsibilities for disaster recovery efforts
3. Recovery Procedures
Detailed procedures to follow for specific recovery situations
4. Debriefing Procedures
Steps to take to evaluate how well the disaster plan worked
5. Insurance Policies
Copies of or extracts from any insurance policies that include disaster coverage
6. Reciprocal Agreements
Copies of any reciprocal agreements with other organizations detailing the services, facilities, and equipment each has agreed to share with the other in case of a disaster

E. Review

1. Roles and Responsibilities
List of staff and their specific responsibilities for reviewing the plan
2. Frequency of review
Stated time frame—for example, periodic, event-driven, or both—for reviewing the plan
3. Testing the plan
Procedures on testing the plan to ensure that it is current
4. Distributing the plan
Procedures for distributing the plan and ensuring that staff know which is the current version

Appendix B

Data Collection Forms

Risk Identification Checklist

This checklist will help you identify potential risks to your records. If a hazard is present, check the box at the left of the form and record additional information about the item in the "Details" column. A properly completed checklist will save time and effort when constructing a disaster management plan.

SITE HAZARDS	DETAILS
Geographic and Climatic Hazards	
<input type="checkbox"/> Floods	
<input type="checkbox"/> Earthquakes	
<input type="checkbox"/> Tornadoes	
<input type="checkbox"/> Hurricanes	
<input type="checkbox"/> Forest fires	
<input type="checkbox"/> Excessive snow	
<input type="checkbox"/> Ice storms	
<input type="checkbox"/>	
<input type="checkbox"/>	
Human Hazards	
<input type="checkbox"/> Power outage	
<input type="checkbox"/> Sprinkler discharge	
<input type="checkbox"/> Fuel or water supply failure	
<input type="checkbox"/> Chemical spills	
<input type="checkbox"/> Explosions (boiler, steam pipe, gas)	
<input type="checkbox"/> Possible terrorist target	
<input type="checkbox"/>	
<input type="checkbox"/>	
Adjacent Environmental Hazards	
<input type="checkbox"/> Chemical industries	
<input type="checkbox"/> Hazardous materials shipping route	
<input type="checkbox"/> Nuclear power plant	
<input type="checkbox"/> Construction site	
<input type="checkbox"/>	
<input type="checkbox"/>	

SITE HAZARDS	DETAILS
Location Risks	
<input type="checkbox"/> Slope	
<input type="checkbox"/> In a flood plain	
<input type="checkbox"/> Large trees nearby	
<input type="checkbox"/> Utility poles	
<input type="checkbox"/> Near highway or railroad tracks	
<input type="checkbox"/>	
<input type="checkbox"/>	
BUILDING HAZARDS	DETAILS
Exterior	
<input type="checkbox"/> Flat roof	
<input type="checkbox"/> Poor roof drainage	
<input type="checkbox"/> Rain gutters obstructed	
<input type="checkbox"/> Poor window seals	
<input type="checkbox"/> History of leaking	
<input type="checkbox"/> Inadequate roof covering and flashings	
<input type="checkbox"/>	
<input type="checkbox"/>	
Interior	
<input type="checkbox"/> Insufficient number of fire extinguishers	
<input type="checkbox"/> Extinguishers not properly charged	
<input type="checkbox"/> Fire alarms not working	
<input type="checkbox"/> Fire alarms not tested regularly	
<input type="checkbox"/> No fire suppression system	
<input type="checkbox"/> Fire exits blocked	
<input type="checkbox"/> No water alarms	
<input type="checkbox"/> Old electrical system	
<input type="checkbox"/> Overloaded electrical system	
<input type="checkbox"/> Old water pipes	
<input type="checkbox"/> Evidence of water stains	
<input type="checkbox"/> Problems with HVAC systems	
<input type="checkbox"/> Dehumidifiers do not drain automatically	
<input type="checkbox"/> Dehumidifiers not checked regularly	
<input type="checkbox"/> Sump pump not working	
<input type="checkbox"/> Problems with furnace or boiler	
<input type="checkbox"/> No sprinkler system in place	
<input type="checkbox"/>	
<input type="checkbox"/>	

BUILDING HAZARDS	DETAILS
Winter Weather Hazards	
<input type="checkbox"/> Clogged rain gutters	
<input type="checkbox"/> Roof and wall vents obstructed	
<input type="checkbox"/> Snow damage on surrounding plants	
<input type="checkbox"/> Unsealed cracks and holes	
<input type="checkbox"/> Broken or cracked windows	
<input type="checkbox"/> Poor building grade	
<input type="checkbox"/> Irregular snow removal	
<input type="checkbox"/> No building checks after major storms	
<input type="checkbox"/> Hydrants not marked or accessible	
<input type="checkbox"/>	
<input type="checkbox"/>	

RISK TO RECORDS	DETAILS
Storage	
<input type="checkbox"/> Open files or volumes on shelves	
<input type="checkbox"/> Unstable shelving	
<input type="checkbox"/> Shelving not anchored to wall or ceiling	
<input type="checkbox"/> Records stored on floor	
<input type="checkbox"/> Shelving not raised 4" to 6" off floor	
<input type="checkbox"/> Records stored in basement	
<input type="checkbox"/> Location vulnerable to flooding	
<input type="checkbox"/> Stored near air conditioners	
<input type="checkbox"/> Stored near restrooms or sewage pipes	
<input type="checkbox"/> Stored near water tanks or pipes	
<input type="checkbox"/> Stored near windows or skylights	
<input type="checkbox"/> Irregular monitoring of storage areas	
<input type="checkbox"/> Stored near furnace or boiler	
<input type="checkbox"/> Stored in garage	
<input type="checkbox"/>	
<input type="checkbox"/>	

RISK TO RECORDS	DETAILS
Security	
<input type="checkbox"/> Storage area not locked	
<input type="checkbox"/> Unsupervised access to records	
<input type="checkbox"/> No monitoring during use of records	
<input type="checkbox"/> Poor key control	
<input type="checkbox"/> Out-of-date records inventory	
<input type="checkbox"/> No records inventory	
<input type="checkbox"/> Fire alarms not marked on floor plans	
<input type="checkbox"/> Fire extinguishers not marked on plans	
<input type="checkbox"/> Door alarms on fire exits not functioning	
<input type="checkbox"/> Alarms do not ring within facilities	
<input type="checkbox"/> Alarms do not notify first responders	
<input type="checkbox"/> No security service contract	
<input type="checkbox"/> Lax testing of alarm system	
<input type="checkbox"/> No emergency lighting system	
<input type="checkbox"/> No water sensors	
<input type="checkbox"/> No emergency generators	
<input type="checkbox"/> Fire exits not clearly marked	
<input type="checkbox"/> Fire exits blocked	
<input type="checkbox"/>	
<input type="checkbox"/>	
Electronic Records	
<input type="checkbox"/> No virus protection on computers	
<input type="checkbox"/> No regular virus protection updates	
<input type="checkbox"/> No regular backup of electronic files	
<input type="checkbox"/> Out-of-date records inventory	
<input type="checkbox"/> No records inventory	
<input type="checkbox"/> No firewall	
<input type="checkbox"/> Infrequent backups	
<input type="checkbox"/> Computers in public or common areas	
<input type="checkbox"/>	
<input type="checkbox"/>	

Completed by: _____ Date: _____

Disaster Response Checklist

This response checklist will help you determine which individuals to contact in case of disaster, each person's assignments, and key sites to use for coordinating the recovery. A completed checklist will save time and effort during an emergency.

PEOPLE TO NOTIFY IN CASE OF A DISASTER			
Internal Contacts	Name	Day Phone	Night Phone
Emergency Coordinator			
Chief Executive Officer			
Building Supervisor			
Records Management Officer			
Records Recovery Team Coordinator			
Information Technology Director			
Recovery Team			
Security			
Building Maintenance			
Finance Officer			
External Contacts	Name	Day Phone	Night Phone
New York State Archives Regional Advisory Officer (RAO)			
New York State Archives Contact in Albany			
Fire Department			
Police Department			
Health Department			
Local Hospital			
Electric and Gas Company			
Water Department			
Insurance Agent			
Legal Advisor			
Electrician			
Locksmith			
Plumber			
Telephone Company			

DISASTER RECOVERY ASSIGNMENTS		
Action	Designate	Alternate
Assess situation		
Determine safety of building		
Determine course of action		
Coordinate recovery plans		
Document damage		
Monitor environment		
Determine salvage priorities		
Authorize disposition of damaged materials		
Provide security and access rights		
Document recovery activities		
Coordinate volunteers		
Contact insurance		
Contact media		
Order additional supplies and materials		
Authorize purchases		
Coordinate refreshments for team		
RECOVERY LOCATIONS		
Location of	Onsite	Offsite
Command post		
Disaster supplies		
Recovery or salvage site		
Duplicate or backup of vital records		
Duplicate building plans		
Duplicate disaster plan		
Salvage team rest area		
Cold site		
Hot site		

Completed by: _____ Date: _____

OUTSIDE SOURCES FOR EQUIPMENT AND SUPPLIES			
Item	On site	Firm and contacts	Phone numbers (day & night)
Freezer space	<input type="checkbox"/>		
Dehumidifiers	<input type="checkbox"/>		
Drying space	<input type="checkbox"/>		
Fans	<input type="checkbox"/>		
Plastic crates	<input type="checkbox"/>		
Pallets	<input type="checkbox"/>		
Plastic sheeting	<input type="checkbox"/>		
Portable sump pump	<input type="checkbox"/>		
Refrigerator	<input type="checkbox"/>		
Wet-dry vacuum	<input type="checkbox"/>		
Unprinted newspaper	<input type="checkbox"/>		
Plastic trash cans	<input type="checkbox"/>		
Plastic trash bags	<input type="checkbox"/>		
Rubber gloves	<input type="checkbox"/>		
Protective clothing	<input type="checkbox"/>		
Respirators	<input type="checkbox"/>		
Fork lift	<input type="checkbox"/>		
Fumigation supplies	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Completed by: _____ Date: _____

Initial Damage Assessment Form

This damage assessment form will help your organization gather information vital to the proper and timely response to emergencies. This information can help you adjust your disaster plan to best deal with an actual disaster.

DISASTER LOCATION		
Address		
Name of Person Reporting		
Telephone		
Date and Time of Report		
Estimated Damage Start Time		
DESCRIPTION OF DISASTER		
<i>Type of damage:</i>		
<input type="checkbox"/> Fire and Smoke		
<input type="checkbox"/> Water:	<input type="checkbox"/> Sewage <input type="checkbox"/> Muddy <input type="checkbox"/> Clean <input type="checkbox"/> Other _____ Source: <input type="checkbox"/> Roof <input type="checkbox"/> Pipe <input type="checkbox"/> Window <input type="checkbox"/> Wall	
<input type="checkbox"/> Collapsed:	<input type="checkbox"/> Roof <input type="checkbox"/> Wall <input type="checkbox"/> Shelves <input type="checkbox"/> Other _____	
<input type="checkbox"/> Infestation:	<input type="checkbox"/> Mold <input type="checkbox"/> Rodent <input type="checkbox"/> Insect <input type="checkbox"/> Other _____	
<input type="checkbox"/> Other _____		
<i>Amount of damage:</i>		
<input type="checkbox"/> Boxes: _____	<input type="checkbox"/> Stacks: _____	
<input type="checkbox"/> Whole Floor: _____ sq. ft.	<input type="checkbox"/> Whole Building: _____ sq. ft.	
<i>Types and quantity of materials involved:</i>		
_____ Bound Volumes	_____ Paper	_____ Photographs
_____ Microfilm	_____ Maps	_____ Computer disks/tapes
_____ Vital Records	Other _____	
<i>General condition of records:</i>		
<input type="checkbox"/> Soaked	<input type="checkbox"/> Still under water	<input type="checkbox"/> Damp
<input type="checkbox"/> Dirty or muddy	<input type="checkbox"/> Scattered on floor	<input type="checkbox"/> Moldy
<input type="checkbox"/> Smoke damage	<input type="checkbox"/> Other _____	

SITUATION AT DISASTER SITE			
Do you have access to the building? <input type="checkbox"/> Yes <input type="checkbox"/> No			
If no, <i>when will you have access?</i> _____			
Are the following available?		If no, <i>When will these services resume?</i>	
Electricity	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Water	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Air conditioning	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Has the source of the problem been halted or controlled? <input type="checkbox"/> Yes <input type="checkbox"/> No			
Are there health hazards at the disaster site? <input type="checkbox"/> Yes <input type="checkbox"/> No			
If yes, please detail			
Are there environmental hazards at the disaster site? <input type="checkbox"/> Yes <input type="checkbox"/> No			
If yes, please detail			
Have you contacted:			
			Time of Contact
Local officials	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Health department	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Insurance company	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Financial Officer	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	
Regional Advisory Officer	<input type="checkbox"/> Yes <input type="checkbox"/> No	_____	

Records Salvage Priority List

List records for salvage in order of priority, taking into account which records are stored near each other. Attach a floor plan to illustrate where the records are located.

	RECORDS	VOLUME	LOCATION
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

Completed by: _____ Date: _____

Appendix C

Sample Disaster Management Plan

The following sample disaster plan from the fictitious Town of North Haverbrook focuses on planning for and responding to records disasters. You may decide to develop a plan with such a focus, but most organizations simply integrate the issue of records into a broader, facilities-wide disaster management plan covering all of an organization's facilities or all areas within the boundaries of a local government. Most likely, your disaster management plan will be more detailed than this one, but this provides a basic outline of a solid plan.

Town of North Haverbrook Disaster Management Plan

1. Policy and Planning

1.1 Introduction

The Town of North Haverbrook is committed to protecting the records and facilities entrusted to its care, as well as its citizens and staff. A disaster management plan is the method the town uses to meet these obligations. Such a plan helps the town evaluate its risks, develop ways to reduce the chances and effects of a disaster, limit loss or damage, and ensure the prompt resumption of essential town services after a disaster.

Records management is a critical element of town governance, and the overall objectives of this plan are to safeguard town records while protecting human life and to guarantee the availability of essential town services in the event of a disaster. Specifically, this disaster management plan documents the policies and procedures related to planning for, preventing, minimizing, responding to, and recovering from records-related disasters. The plan is general in nature and designed to function in response to any disaster, regardless of type or scale.

1.1.1 Assumptions of This Plan

This plan cannot ensure that the town will avoid all disasters or protect all records in the event of a disaster. The town assumes, however, that a plan can prevent or limit the effects of any potential threats by identifying those risks beforehand. With careful planning, the town will reduce a disaster's impact on its records and services. The town clerk will ensure the incorporation of elements of this records-focused plan into the overall emergency operations strategies for the Town of North Haverbrook.

1.2 Glossary of Terms

This glossary defines the technical disaster management terms used in this plan.

archival record a record with continuing value, primarily one scheduled as permanent in the State Archives' *Records Retention and Disposition Schedule for Municipalities (MU-1)*

assumption a basic belief about a potential disaster situation used to develop a disaster management plan

checklist test a method of analyzing a disaster recovery plan by verifying that lists of information in the plan, such as phone numbers and emergency equipment, are accurate

crisis a serious event that, if not addressed appropriately, would likely reduce an organization's ability to operate

disaster a serious event requiring an immediate response to prevent a lapse of essential business functions (See "records disaster")

disaster management a system of measures used to prevent, detect, contain, respond to, and recover from events that threaten the ability of an organization to function

disaster prevention a pre-determined system of measures used to avert, detect, or contain events that threaten the ability of an organization to function

disaster recovery a pre-determined system of measures used to restore an organization's critical business functions, including the usability of its records

disaster recovery plan a document that outlines actions to take to respond to a disaster, salvage records and equipment, and resume business operations

disaster recovery team a team of people trained and prepared to take control of response and recovery in the event of a disaster

disaster response a pre-determined system of measures used to react to events that threaten the ability of an organization to function and that includes preliminary assessment of the situation and the development of a plan of action to recover records and restore business functions

essential services official business functions that an organization must maintain before, during, and after a disaster

mitigation the reduction of the chances that a disaster will occur, and the reduction of its negative effects if one does occur

record information, in any format, that is created or received by an organization in the formal operation of its responsibilities

records disaster a serious event requiring an immediate response to prevent the irretrievable loss of vital or archival records

records management the systematic control of all records in an organization throughout their life cycles

risk a potential source of danger that could expose an organization to a lapse in business functioning or to the loss of vital or archival records (Also called “threat” or “hazard”)

simulation test a method of analyzing a disaster recovery plan by approximating a specific disaster scenario and running through a drill of the plan

tabletop test a method of analyzing a disaster recovery plan by having a disaster recovery team discuss and then evaluate the actions they would take in the event of a specified disaster

vital record a record essential for the protection of the financial well-being of an organization, its legal rights, and the rights of its citizens and employees; a record without which an organization could not conduct its business

1.3 Disaster Management Policy

1.3.1 Purpose

The town clerk as records management officer is responsible for developing and implementing policies and procedures to ensure the maintenance, accessibility, and preservation of town records. This disaster management policy defines how the town will develop and maintain its disaster management plan for the protection of vital and archival town records.

1.3.2 Scope

This policy covers the records of all town departments, whether stored in town offices, onsite records storage, or offsite.

1.3.3 Policy

The Town of North Haverbrook will demonstrate a commitment to effective disaster management by ensuring the following:

- The annual budget contains adequate financial support to maintain and implement a suitable disaster management program.
- The town has reasonable and effective disaster management policies and procedures in place.
- The town's records management office, with the cooperation of individual departments, develops priorities for the management and protection of town records.
- The town's disaster recovery team carefully assesses and re-evaluates risks to its records and its essential services.
- Town personnel periodically evaluate disaster control requirements and upgrade these when necessary.
- The town emphasizes disaster prevention over response and recovery.
- The town clerk assigns disaster management responsibilities appropriately and ensures that those assigned understand their responsibilities.
- The town clerk ensures that the disaster recovery team receives appropriate and regular training.
- The town clerk ensures the periodic testing of the disaster response plan and monitoring of preventive measures.
- The town clerk ensures that all personnel are familiar with the disaster management policy and plan.
- The town clerk ensures that the disaster management policy and plan are integrated into the town's overall emergency planning strategies.
- The town clerk ensures the annual review of the disaster management policy and plan.

1.3.4 Promulgation of the Policy and Plan

The town records management office will distribute the disaster management policy and plan to all town staff.

1.3.5 Monitoring and Review

Since the disaster management policy and plan are living documents, the town clerk will oversee their annual review and update them when needed. (See Section 5, "Review," for more details on these activities.)

1.4 Roles and Responsibilities

The town clerk and the fire marshal have the greatest responsibility for disaster management. The town clerk, who is also the town's records management officer, is responsible for the care and general management of all records in the town. The fire marshal is responsible for ensuring that town facilities are free of risks that might cause fires, that appropriate protections are in place to contain any fires that do occur, and that there are plans in place for the safe and efficient evacuation of people from town facilities in the case of a fire. The following policy development tasks must take place during the initial planning phase and be performed again later for plan maintenance.

The town clerk will

- verify that all components of the disaster management plan are current and accurate
- update and revise the plan annually or as needed
- maintain secure and accessible electronic and paper copies of the disaster management plan offsite
- schedule regular disaster response and recovery training and ensure that appropriate staff attend
- distribute, as appropriate, key sections and updates of the plan to town officials and to emergency response units including the police and fire departments
- identify the annual budget to maintain the plan
- test the plan on an annual basis

The fire marshal will

- advise the town clerk of any information that may affect disaster management planning
- integrate this disaster management plan into the Town of North Haverbrook's emergency operations plan

2. Prevention

2.1 Introduction

Prevention is key to effective disaster management. It is always better to prevent or minimize an incident than to implement response, salvage, and recovery procedures. Many town records are irreplaceable, so the town will address this component of the plan as part of an annual plan review and through regular maintenance practices.

Prevention means anticipating and controlling potential hazards to manage records. Correcting minor or chronic problems before they become serious can prevent incidents from becoming disasters that

destroy or damage records. Repairing damaged records can be expensive and time-consuming, and it deprives the town of access to records, thereby reducing the town's ability to provide an expected level of service.

For the purposes of prevention, the town will undertake the following routine activities:

- conduct building inspections, in cooperation with building maintenance personnel and the fire marshal, to ensure that facilities do not and will not negatively affect the physical condition of records
- inventory the town's records to identify those vulnerable to environmental risks such as high temperatures
- review and improve records access, care, handling, storage, and disposition practices

Building floor plans that are part of the disaster management plan must include records salvage priorities so that staff can quickly locate valuable records in the event of an actual disaster.

2.2 Roles and Responsibilities

The town clerk will

- ensure that staff manage records in accordance with State Archives guidelines
- guarantee that the storage of fragile records will be unlikely to cause their damage or destruction
- provide additional security and physical protection, if necessary, for vital, important, and archival records
- review and update the records management needs assessment, putting into place new or upgraded controls and procedures as required
- bring to the attention of building maintenance personnel or the fire marshal any problems that may affect records

The fire marshal will

- verify that existing building controls such as fire and security alarms are working properly
- evaluate security, water and fire protection measures on a regular basis to confirm that they are adequate to protect records
- bring to the attention of the town clerk any potential threats to records
- stay informed of severe weather and geological conditions
- communicate all pertinent information to the town clerk as soon as possible

Building maintenance personnel will

- undertake monthly building inspections
- take corrective actions to eliminate deficiencies identified in building inspection reports
- advise contractors of what precautions to follow when renovating or repairing facilities
- communicate all pertinent information to the town clerk as soon as possible

Records management staff and others with records responsibilities will

- manage records according to State Archives guidelines
- implement and maintain regular backup procedures for electronic records and store these backup copies in a safe and secure location offsite
- prevent unauthorized access to electronic records by securing equipment and storage facilities, installing computer firewalls and virus detection software, limiting access to LAN servers, and adopting other security measures where appropriate
- bring to the attention of the town clerk any problems that may affect records

2.3 Site Maintenance and Inspection

An essential part of this disaster plan is to reduce the chances that the town will suffer a disaster. For that reason, the head of maintenance will ensure that all town facilities are inspected for potential risks at least quarterly using the town's risk identification checklist.

3. Response

3.1 Introduction

The town must respond to any disaster in a quick and organized manner. Planning an appropriate response is always difficult because of the unique nature of every disaster. Since the town cannot schedule disaster response ahead of time, it cannot be sure all members of the disaster recovery team will be available to help. Additionally, response can entail many hours of difficult physical work in potentially dangerous situations, so town personnel must be careful to ensure their own safety during any disaster response.

3.2 Roles and Responsibilities

The first person to discover a records disaster or to determine one is imminent will

- contact the town clerk and fire marshal to initiate the disaster response
- contact the deputy town clerk if the town clerk or fire marshal is not available
- contact appropriate emergency response units (fire, police, ambulance), if necessary

The town clerk will

- serve as the leader of the disaster recovery team
- ensure that the team contacts appropriate emergency response units
- contact the first person on the disaster recovery team's phone tree, and indicate where and when team members will congregate
- retrieve the copy of the disaster plan kept at the town clerk's residence
- retrieve the disaster response supplies kept at the town clerk's residence, including communication devices like cell phones and two-way radios
- arrive at the scene as quickly as possible
- begin the initial damage assessment
- determine methods of response to address this particular disaster
- contact any professionals needed to help with the response (including freeze-drying companies and the State Archives' Regional Advisory Officer)
- organize and direct the disaster response team
- oversee the general disaster response as it relates to records
- communicate and coordinate activities with official disaster response units (fire, police, and ambulance)

The fire marshal will

- serve as the deputy leader of the disaster recovery team, and serve as the leader in the absence of the town clerk
- retrieve the copy of the disaster plan kept at the fire marshal's residence
- retrieve the disaster response supplies kept at the fire marshal's residence, including communication devices like cell phones and two-way radios

-
- arrive at the scene as quickly as possible
 - help the town clerk complete the initial damage assessment
 - help the town clerk devise the methods of response for this particular disaster
 - keep in frequent contact with the town clerk during the response
 - designate a media representative who will answer any questions and provide information on the state of the response

The disaster response team will

- contact the next person on the disaster response team's phone tree; if that person is not available, contact the following person on the tree
- arrive at the scene by the time and at the location indicated
- follow the directions of the town clerk and fire marshal

3.3 Actions to Take in Case of a Disaster

3.3.1 Security

First, establish security so that only authorized personnel enter the affected areas. Establish a cordon around the affected area, staffed by police or members of the disaster response team, as appropriate. Limit the number of people entering the area to reduce the chances of injury and pilfering.

3.3.2 Stabilization of the Area

Before attempting to recover any records, first determine the source of the problem. Wait until all fires are quenched, excess water is drained, and unstable structures are dismantled. Do not enter any structure until the fire chief tells the town clerk that the building is safe to enter.

If the building is not safe for town staff to enter, the town clerk will work with the fire chief to determine whether firefighters can use the floor plans and records salvage list to retrieve the town's most valuable records. If the building is too dangerous for anyone to enter, the town clerk will develop a salvage plan with the fire chief.

If the area is flooded, first clear any drains to empty the water. Keep in mind that water conducts electricity, so turn off the power before entering a room with standing water.

After removing the water, keep the temperature below 65 degrees Fahrenheit, which will be cold enough to retard mold growth. Run fans to circulate air and dry out wet areas. Run dehumidifiers to reduce dampness. Remove all discardable, wet materials such as carpets, paper supplies, and empty storage cartons.

3.3.3 Stabilization of the Records

Use rubber gloves to handle all materials, and wear appropriate face masks if mold is present in the area. Immediately use the “Records Salvage Priority List” to identify and relocate any vital or archival records. Begin with any records threatened with further damage because they are submerged, about to tumble to the ground, or otherwise vulnerable. If any boxes are falling apart, temporarily store the records in plastic containers or standard cubic-foot cardboard boxes (if plastic ones are not available). Move all reboxed records to a dry, sheltered location. If records are wet, do not leave them permanently in the boxes used for moving; either dry them under fans or contact a freeze-drying specialist immediately.

3.4 Disaster Response Checklist

Insert a copy of the Disaster Response Checklist to help you determine which individuals to contact, how to contact them, and their initial assignments in case of a disaster.

3.5 Emergency Equipment Inventory

Insert a copy of your emergency equipment inventory, which will indicate the availability and location (onsite or offsite) of supplies and equipment that support disaster response, including fire extinguishers, smoke alarms, and shut-off valves.

3.6 Initial Damage Assessment Form

Insert a blank copy of the initial damage assessment form, which will help your organization gather preliminary information about the extent of a disaster.

3.7 Records Salvage Priority List

Insert a records salvage priority list that details the locations of the archival and vital records to save in the event of a disaster.

3.8 Floor Plans and Area Maps

Insert detailed floor plans of all buildings maintained by the organization, indicating the locations of records, and area maps that indicate the location of important resources such as water mains and hydrants.

4. Recovery and Business Continuity

4.1 Introduction

The line between disaster response and recovery is not always distinct. Response relates to all actions required to assess the extent of the disaster, identify methods needed to save records, and protect

property and human life. Recovery relates to actions taken to resume the normal business activities of the town.

4.2 Roles and Responsibilities

The town clerk will

- verify the availability of promised temporary work space at the Town of Ogdenville
- ensure the availability of adequate furniture to conduct town work

The director of information technology will

- verify the availability of adequate computer equipment and telecommunications at the temporary Town of Ogdenville site
- acquire rented computer equipment
- set up adequate computer systems to run essential town services

4.3 Recovery Procedures

Insert detailed procedures for specific recovery situations. These might include recovery procedures in cases of total destruction of facilities and procedures in cases of partial damage to a single facility.

4.4 Debriefing Procedures

Steps to take after recovery to evaluate how well the disaster plan worked.

4.5 Insurance Policies

Copies of or extracts from any insurance policies showing disaster coverage.

4.6 Reciprocal Agreements

Copies of any reciprocal agreements with other organizations detailing the services, facilities, and equipment each has agreed to share with the other in case of a disaster.

5. Review

5.1 Introduction

Disaster management requirements will change over time, so the Town of North Haverbrook will review this plan annually to guarantee its continuing effectiveness and relevance to the town's overall emergency operations.

5.2 Roles and Responsibilities

The town clerk will be responsible for calling together the disaster response team to review the disaster plan.

The head of maintenance is responsible for keeping town facilities in good condition to minimize natural or structural risks that might invite disasters.

5.3 Frequency of Review

The disaster response team will review the disaster plan in two separate ways:

5.3.1 Annual review

Once a year, the disaster response team will review the disaster response plan in its entirety to ensure that it is up to date. The team will make the necessary changes it identifies at that time.

5.3.2 Event-driven review

After any disaster response and recovery, the disaster response team will review the disaster and its response. The team will use that information to revise the disaster plan, as necessary.

5.4 Testing the Plan

The town clerk is responsible for testing the plan to ensure that it is a useful tool for the town. Testing methods will include tabletop testing at each annual review and occasional, unannounced simulation tests.

5.5 Distributing the Plan

After any modification to the plan, the town clerk will distribute amended copies to all town staff and ensure the storage of copies offsite. The town clerk will mark all updates to ensure that the disaster recovery team does not inadvertently use old information.

Appendix D

Glossary of Disaster Management Terms

access permission, opportunity, and ability to use a record

activation the process of putting a disaster recovery plan into action

alternate site a location, other than the normal facility, used to conduct critical business functions in the event of a disaster

archival record a record that should be kept permanently because of its administrative, legal, fiscal, or research value; also called “historical record”

assumption a basic belief about a potential disaster situation used to develop a disaster management plan

back up (verb) to copy an electronic record to ensure its information will not be lost, often while compressing data to save space

backup (noun) a copy of an electronic record, maintained to protect the information from loss and often compressed to save space

business continuity the resumption and maintenance of regular business activities after a disaster

checklist test a method of analyzing a disaster recovery plan by verifying that lists of information in the plan, such as phone numbers and emergency equipment, are accurate

cold site an alternate site that has no equipment or resources except for basic climate control and adequate space

crisis a serious event that, if not addressed appropriately, would likely reduce an organization’s ability to operate

damage assessment the process of determining the extent of destruction following a disaster and of planning upcoming steps

disaster a serious event requiring an immediate response to prevent a lapse of essential business functions (*See* “records disaster”)

disaster management a system of measures used to prevent, detect, contain, respond to, and recover from events that threaten the ability of an organization to function

disaster prevention a pre-determined system of measures used to avert, detect, or contain events that threaten the ability of an organization to function

disaster recovery a pre-determined system of measures used to restore an organization’s critical business functions, including the usability of its records

disaster recovery plan a document that outlines actions to take to respond to a disaster, salvage records and equipment, and resume business operations

disaster recovery software a computer program designed to help an organization write a comprehensive disaster management plan

disaster recovery team a team of people trained and prepared to take control of response and recovery in the event of a disaster

disaster response a pre-determined system of measures used to react to events that threaten the ability of an organization to function and that includes preliminary assessment of the situation and the development of a plan of action to recover records and restore business functions

electronic record

(definition from the Electronic Signatures and Records Act) “information, evidencing any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities”

(simple definition) a record that is in electronic form

essential services official business functions that an organization must maintain before, during, and after a disaster

facility a permanent location containing the equipment, supplies, and telecommunication lines used by an organization to conduct its business

Federal Emergency Management Administration (FEMA) the department of the United States’ government responsible for directing response and recovery in the face of catastrophic disasters of national significance

FEMA See “Federal Emergency Management Administration (FEMA)”

firewall a security system that uses hardware and/or software mechanisms to prevent unauthorized users from accessing an organization’s internal computer network

freeze-drying the process of freezing water-soaked documents and vacuuming away the moisture as they dry

hazard See “risk”

historical record a record that must be kept permanently because of its administrative, legal, fiscal, or research value; also called “archival record”

hot site an alternate site that includes all the equipment, data, and resources deemed necessary to resume business functions affected by a disaster

human threat any risk of disaster that can be caused by the actions of people, including computer hacking, vandalism, and terrorism

information security the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional

information technology (IT) the system for managing the entire range of computing, telecommunications, and information services; sometimes called “information services” (IS) or “management information services” (MIS)

LGRMIF See “Local Government Records Management Improvement Fund (LGRMIF)”

Local Government Records Management Improvement Fund a dedicated fund used to improve records management and archival administration in New York State’s local governments and comprised of fees collected by county clerks and the New York City Register for the recording of selected documents

loss the business resources destroyed or damaged as a result of a disaster, including records, facilities, operational capability, human life, and public image

malicious code any software that is intentionally introduced into a system with an unauthorized purpose

mitigation the reduction of the chances that a disaster will occur, and the reduction of its negative effects if one does occur

natural threat an event in nature that can cause a serious disruption to an organization's business functions

non-record an information format (such as an outside publication, blank form, or instruction manual) that is not an official record and therefore does not require retention

obsolete record a record that has met its retention period, is no longer useful to the organization, and that may be destroyed legally

offsite storage a secure location, remote from the work location, used to store inactive, vital, or archival records

password a character string usually selected by a user, known to the computer system, and used in conjunction with an associated username to identify the user and allow access to the system

privacy the expectation that personal information will be protected from unauthorized disclosure

RAO *See* "regional advisory officer (RAO)"

reciprocal agreement a contract between two similar organizations that permits either one to use the other's facilities or resources in the event of a disaster

record

(informal definition) information, in any format, that is created or received by an organization or received in the formal operation of its responsibilities

(legal definition for local governments in New York State) any book, paper, map, photograph, microphotograph or any other information storage device regardless of physical form or characteristic which is the property of the state or any state agency, department, division, board, bureau, commission, county, city, town, village, district or any subdivision thereof by whatever name designated in or on which any entry has been made or is required to be made by law, or which any officer or employee of any said bodies has received or is required to receive for filing

(legal definition for state agencies in New York State, plural) all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by any agency of the state or by the legislature or the judiciary in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities, or because of the information contained therein

records disaster a serious event requiring an immediate response to prevent the irretrievable loss of vital or archival records

records management the systematic control of all records in an organization throughout their life cycles

records manager the person in an organization whose primary responsibility is the systematic management of official records

records retention *See* “retention”

records retention and disposition schedule a list of records series titles that indicates the length of time to maintain each series; also called a “records schedule” or “retention schedule”

records schedule *See* “records retention and disposition schedule”

records series a group of related records (such as minutes of a board, payrolls, or purchase orders) that are normally used and filed as a unit and that often have the same retention requirements

regional advisory officer (RAO) a representative of the New York State Archives who provides records management advice to local governments and state agencies in a particular region of the state

remediation actions taken to improve the conditions of facilities and records after a disaster has occurred

retention the act of keeping records for a specific amount of time given their administrative, fiscal, legal, or historical value and use; also called “records retention”

retention schedule *See* “records retention and disposition schedule”

risk a potential source of danger that could expose an organization to a lapse in business functioning or to the loss of vital or archival records; also called “threat” or “hazard”

risk identification checklist a questionnaire used to assess the possible threats to the records, security, information systems, or personnel of an organization

risk management the discipline that includes disaster management and ensures that an organization reduces its level of risk to a reasonable level

salvage procedure an action taken to recover any records or equipment that may have been damaged during a disaster

schedule

(noun) *See* “records retention and disposition schedule”

(verb) to determine and formalize the retention period for a records series

security the protection of records by controlling which users can access which documents and for what purpose

self-insurance the practice an organization uses to manage its own exposure to risk by ensuring that it has put aside enough capital to meet any expected losses

SEMO *See* “State Emergency Management Office (SEMO)”

series *See* “records series”

simulation test a method of analyzing a disaster recovery plan by approximating a specific disaster scenario and running through a drill of the plan

State Archives the New York State Archives, the state agency that preserves and provides access to the historical records of state government and that provides records management and archives services to local governments, state agencies, and non-profit historical records repositories

State Emergency Management Office (SEMO) the unit of New York State government responsible for directing response and recovery in the face of catastrophic disasters of state significance

tabletop test a method of analyzing a disaster recovery plan by having a disaster recovery team discuss and then evaluate the actions they would take in the event of a specified disaster

threat *See* “risk”

virus a piece of computer code that, once loaded onto a computer, carries out mischief or destruction against a computer system

vital record a record essential for the protection of the financial well-being of an organization, its legal rights, and the rights of its citizens and employees; a record without which an organization could not conduct its business

warm site an alternate site that is only partially equipped (*See also* “hot site”)