Essential Records Manual

SECURITY BACKUP, DISASTER PREPAREDNESS RESPONSE, AND RECOVERY

Office of the Secretary of State
Division of Archives and Records Management

Acknowledgments

This manual was prepared by Cary Information Consulting. Authors of this manual wish to acknowledge the following people and organizations for their assistance: Barbara Benson, Director of Records Management Services, University of Washington; Mary Campbell, Records Officer, Starbucks Corporation; Randy Stilson, The Evergreen State College; George Helton, Yakima County Information Services Department; Mary Beth Sweeten, Disaster Recovery Coordinator, Washington State Department of Information Services; Jeanette Lomax, Emergency Management Division, Washington State Military Department; Jeff Benson, National Archives and Records Administration; and Mike Storino, Munters Moisture Control Services.

Special thanks to the Virginia State Library for permitting use of information from its “Disaster Preparedness and Recovery Workbook.” Several templates in the appendices of this manual were abstracted from that workbook. And again, a special thanks to Barbara Benson at the University of Washington for permission to adopt portions of her outlined recovery procedures.

INTRODUCTION

1. PURPOSE

The purpose of this manual is to help local agencies protect their essential records information from damage, loss, or theft.

First, the manual helps you:

- Define your essential records and protect them.
- Conduct a risk analysis.
- Reduce the chances of a records damage, loss or theft.
- Produce a Records Disaster Recovery Plan.

Second, when a disaster does occur, the manual:

- Guides you through a disaster and provides recovery options.
- Serves as a technical and self-help guide.

2. HOW TO USE THE MANUAL

The manual provides detailed, step-by-step help and instructions for essential records protection, as well as procedures for prevention, preparedness, disaster response, and recovery. Parts I, II, and III of the manual are keyed to templates in the Appendices.

A template consists of blank forms and instructions. Each template comprises a part of the plan. Most organizations will not need to use every template. Organizations should choose those templates that apply to them, and add any new forms or written procedures that may not be covered. When an organization completes this process, it will have a records disaster plan. Of course, the plan will need to be tested and revised as necessary.

For immediate information on saving damaged records, see Appendix C.

Additional help in writing the plan may be obtained from the Archives Division, which periodically presents disaster preparedness workshops across the State. Additional information may be obtained at http://www.secstate.wa.gov/archives/

3. BASIC CONCEPTS

The following basic concepts are listed in summary form. They will be described in greater detail in Parts I, II, and III and in the appendixes.

A. Public Records: The term “Public Records” applies to any paper, correspondence, form, bound volume, film, magnetic record, drawing, or other document, regardless of media, that has been created or received by any state or local government agency during the course of public business (RCW 40.14.010).

B. Records management: Records are public property. Like any asset, they must be managed efficiently and prudently over their life cycle. Records management includes authorities, responsibilities and procedures for managing an agency’s records and information. Practicing good records management can dramatically reduce the impact of a disaster and the response and recovery efforts.

C. Essential Records: Essential records, sometimes called vital records, are the records necessary for the continuity of operations during and following a disaster. See

Part I and Appendix B for detail. They are records an agency must have to maintain one or more of the following vital functions:

- Document the agency's legal authorities, rights and responsibilities (ordinances, resolutions, minutes, rules, and regulations etc.).
- Resume or maintain operations in a disaster or emergency situation.
- Document the rights of individuals (deeds, mortgages, court case files).

D. Risk Assessment: A disciplined approach to evaluating threats to records, potential impact of damage, and prioritization of protection, response and recovery efforts (covered in Part I).

E. Planning and Preparedness: The best way to avoid records disasters or to mitigate their effects is to plan in advance. An Essential Records and Records Disaster Plan, covered in Part II and Appendix B of this manual, will set out policy, authority, procedures, resources, and techniques for dealing with disasters to records.

F. Response and Recovery: These activities happen after a disaster or emergency occurs. Response is what is done during and immediately following a disaster to minimize damage and resume emergency operations. Recovery covers the process of salvaging records and information systems and putting them back into full and normal operations.

G. Stages of Essential Records Protection: Planning, protection and response activities logically occur in phases. The manual is organized according to these phases:

(1) Prevention: This phase is covered in Part I and Appendix B.
(2) Planning: How to develop a plan is covered in Part II and Appendix A.
(3) Response and Recovery: This phase is covered in Part III and Appendix C.

4. ROLE OF THE ARCHIVES DIVISION

Chapter 40.10 of the Revised Code of Washington was enacted to help agencies prepare for threats. It mandates that:

> "The State Archivist of Washington shall coordinate the essential records protection program and shall carry out the state emergency plan as they relate to the preservation of essential records."

The Archives Division of the Washington State Office of the Secretary of State (OSOS) has targeted specialized guidance and technical support services to assist in the protection of essential government records. One element is this Disaster Prevention, Preparedness and Recovery Manual. Another is the presentation of specialized workshops on essential records and disaster recovery to local agencies. Additional help and information is provided on compact disks (CDs) and on the OSOS web site. The division also provides on-site technical assistance to state and local government agencies undergoing disaster recovery efforts.

5. DISASTERS

Disasters of all kinds occur almost every day. They range from the extreme example of the New York World Trade Center tragedy in September 11, 2001, and the Puget Sound earthquake of 2001, to smaller local disasters such as a burst water pipe in a file room. They come in all forms including flood, fire, earthquake, wind, and man made events including sabotage and terrorism. One of the primary responsibilities of government is to prepare for disasters and lead the public response and relief effort.

A disaster is generally considered an event that is beyond the powers of the first responders to prevent or control the situation, resulting in loss of life and property. Records disasters are a sub-set of disasters in general. For the purpose of this manual, a records disaster is defined as:

> "The loss or unavailability of records or data that disrupts an organization's functions or results in loss or threat of loss to rights and assets of the organization or the public."

The definition is relative. It could refer to the destruction of 1,000 boxes or one box, or the loss or destruction of a computer hard drive that has not been backed-up. Note that the definition includes unavailability of records as well as loss or destruction because there are times when the loss of data for even a period of days is unacceptable.

6. TYPES OF DISASTERS

There are many causes of records disasters such as earthquakes, floods, storms, fires, broken water mains, sabotage, and terrorism. In Washington, these causes result in relatively few categories of damage to physical records:

- Water damage (may result in progressive further damage such as mold). Water damage is by far the most common type of damage.
- Fire damage (charred and burned, usually accompanied by water damage).
- Contamination (substances poured onto records such as gasoline, PCBs from transformers, sewage from broken pipes, etc. They are often accompanied by water damage).
- Unavailability (building may be unsafe, cannot get at the records right away).

The causes of damage to electronic records include the foregoing plus other causes such as:

- Power failure
- Equipment failure
- Software problems
- Human caused events such as virus infection
- Human error

7. IT CAN HAPPEN TO YOU!

In Washington State in recent years, there have many instances of records damage from a variety of causes including fire, flood, earthquake, contamination, computer viruses, and intentional sabotage. These range in scale from major disasters damaging thousands of boxes, to mid-size disasters affecting a few hundred boxes, to small but critical threats to a few boxes of important records. Examples include:

- Okanogan County Superior Court: An attempt was made in 2002 to fire bomb county court files. Fortunately an alert individual smelled the fumes before the bomb went off. However, the combustible fluids poured on the files contaminated them and they had to be recovered.

- Seattle Housing Authority: During the Christmas holiday a water pipe broke directly over a set of 12 boxes in the record center and soaked them. The boxes contained a special collection of original copies of deeds and other proof of ownership documents for hundreds of houses, buildings, and other real property. The records manager was called at home. There was no one available to advise her on what to do, but she had a disaster recovery chapter of her file manual. Following the recommended procedure, she immediately froze the records and restored them later by freeze-drying and thereby saved the records.

PART I -- PREVENTION

Part I of the manual covers steps that can be taken to reduce the scope of a disaster or prevent it from happening at all. It includes chapters on essential records, records management, electronic records, and risk analysis.

CHAPTER 1: ESSENTIAL RECORDS PROTECTION

ESSENTIAL RECORDS –DEFINED

Records necessary for the continuity of government operations during or following a disaster, and which support one or more of the following:

- Document the agency's legal authorities, rights, responsibilities, and financial status.
- Are necessary to resume and restore operations.
- Document the rights and obligations of its employees and the citizens it serves.

Essential Records can be on any media or format that contains information that must be protected against loss, including paper, photographic images, microfilm, electronic data systems, electronic images, maps and drawings, or any other media used for recording information of all types. Typically they are a small portion of an agency's records, but in some agencies most of the records may be essential, such as courts and county recorders.

Examples:

- Records of governance (council/commissioners' minutes, ordinances, and resolutions.)
- As-built facilities plans and drawings
- Property ownership records – deeds, leases and titles

WHY IS THE IDENTIFICATION AND PROTECTION OF ESSENTIAL RECORDS SO IMPORTANT?

Identification and protection allow you to:

- Respond to a disaster affecting records.
- Minimize disruption of operations after an emergency.
- Rapidly restore government services.
- Reduce the economic impact of a disaster.

It is simply good business practice. While there is an up-front cost and effort to protect essential records, it will usually be far less than recovering damaged records after a disaster.

LEGAL IMPLICATIONS

Identification and protection of essential records is also written into law and regulation.

- Chapter 38.52 RCW requires state and local agencies to have Emergency Management Plans.
- EMD (the Division of Emergency Management of the State Military Department) issues guidelines for local agencies to prepare those plans, including essential records protection.
- The Essential Records Act (RCW 40.10) directs state agencies to identify and protect their essential records, and sets forth specific actions for doing so. Local agencies are responsible for doing the same.

ESSENTIAL RECORDS PROTECTION

An Essential Records Protection Plan consists of **five basic elements**:

1. **Identify** which records are essential to your organization.

2. **Decide** which method you are going to use to protect each essential records series.

3. **Develop an Essential Records Schedule** that will list the records series deemed essential, indicate how they are protected, and identify who is responsible for protecting them.

4. **Implement** the protection measures selected for each record series.

5. **Test** periodically.

STEP 1 - IDENTIFYING ESSENTIAL RECORDS

There are several approaches to identifying essential records.

a. Identify the key functions of your agency.

b. Identify essential records series for each function using:
   - Agency functional and organizational charts.
   - Essential Records Schedule template in Appendix B-2.
   - The Washington State General Records Retention Schedule for Agencies of Local Government (See Appendix B-3 for a listing of these record series).
   - The General Records Retention Schedule approved specifically for your type of agency, such as County Auditor, County Clerk, County Treasurer, Health Department/District, Hospital District, Law Enforcement, and School District.

c. If you are still in doubt as to whether a record is essential the following questions may help:
   - What will be the consequences if these records are lost?
   - What will be the cost in terms of time, labor, and money if these records have to be reconstructed?
   - How rapidly will these records have to be reconstructed before serious damage is done to the operation, three months, a month, a week, day or hour?
   - Can these records be readily replaced from another source, agency, office, etc?
   - Are these records already duplicated or replicated in another form?
   - If in an electronic database, is the information sufficient to substitute for the original record?

STEP 2 - SELECTING METHODS OF PROTECTION

There are a several strategies and methods for protecting essential records from disaster. They range from simple steps, using existing file equipment and filing practices, to duplication and mirrored sites for electronic records. Each strategy or method represents a different level of protection and cost. The methods are not mutually exclusive.

Best Strategy: Experts agree the best strategy for protecting all types of essential records is duplication and off-site storage. However, there are low cost alternatives that can provide acceptable levels of protection for many records, depending on their value and level of risk. Part of the task of essential records planning is to assess the level of risk. See Part I, Chapter 4 Risk Analysis.

STRATEGY A: SIMPLE WAYS TO PROTECT ESSENTIAL RECORDS ON-SITE

1. **Transfer essential records to a non-current records storage center as soon as possible.** Reduce the time they are kept in office space to the minimum, consistent with retrieval needs.

2. **Locate essential records.** Mark their location on a floor plan. Put a copy of the floor plan in your records disaster plan. Give a copy to your agency's disaster recovery team members and the fire department.

3. **Keep essential records separate from other records**. They will be easier to find during an emergency.

4. **Keep essential records close together**. They will be easier to find and move.

5. **Locate essential records as close to the door as possible.** Easier to remove quickly.

6. **Keep essential records folders, documents and disks off desks**. As much as possible, put them away in file cabinets. Papers and files on desks or credenzas are extremely vulnerable to fire and water damage. These records are typically current and extremely valuable to operations.

7. **Keep essential records off the floor.**

8. **Keep essential records in metal drawer file cabinets**. File cabinets protect records better than open-shelf files since they can be closed. Shelf files that have doors that close are better than open shelf cabinets but not as safe as drawer type cabinets. Fire resistant cabinets offer even better protection but are expensive.

9. **Keep essential records out of bottom drawers.** Bottom drawers are more likely to be damaged in a flood. It is also better not to use top drawers, as they are apt to be wetter and hotter.

10. **Put special labels on essential records file cabinets.** The labels should be metal and readable even after a fire. Ideally they should be riveted onto the cabinets.

STRATEGY B: FACILITY PROTECTION AND SECURE ON-SITE STORAGE

On-site storage means storing essential records in proximity to the office.

Vaults, safes, and fire-resistant file cabinets offer protection against fire, theft, and vandalism. Vaults and safes and some file cabinetry are rated for fire resistance. A three-hour rating is often suggested, however hours of protection decrease as the temperature of the fire increases.

Such cabinets may not provide complete protection against a major conflagration or flood and are expensive.

Secure file rooms with smoke and intruder detection, sprinkler systems, compact or moveable shelving, and key control offer another on-site protection option.

The major drawback of all on-site storage is that it relies entirely on the ability to physically protect the original record. The best way to determine the viability of on-site storage is to make both a risk analysis and a physical threat assessment. See Chapter 4, Risk Analysis and Appendix B Risk Assessment and Prevention Plan Templates.

STRATEGY C: DUPLICATION AND OFF-SITE STORAGE

There are a number of methods for duplicating essential records. Each has advantages and disadvantages.

Essential records can be copied to paper, microfilm, electronic, or optical media. In some cases the informational content is essential rather than the document itself. The information may already be contained in an electronic system and thus “duplicated“ in an electronic form.

Do not store security duplicates at the same location as the original essential record. Duplicates should be stored off-site.

Paper Duplication

Advantages:

- Minimum chance of the primary and the security duplicate both being destroyed.
- Easy to do and can be done in the normal course of business.
- May be sent off-site using a commercial records storage service or an agency facility. The transfer process can be the same as the process for sending inactive records, provided the transmittal documents identify the box as containing “essential records.”
- Does not require special equipment to read.
- May already exist as copies sent to another office or offices for informational purposes. One or more of these copies can be designated as security copy.

Disadvantages:

- More expensive to produce and ship than microfilm.
- Difficult and cumbersome to keep an active duplicate paper file up to date.
- Becomes voluminous and costly to store.
- Does not work well if the designated office is on the same floor or in the same building as the office that houses the original record.
- Duplicates are decreasing as a viable method of protection except for very small collections of essential records with short retentions.

Microfilm

Advantages:

- Microfilm is nearly 100 times more space efficient than paper.
- Microfilm is less costly to produce, ship, and store than paper.
- Microfilm is as durable as or more durable than paper.

Disadvantages:

- Cost efficiency is dependent on batching and filming many documents at once, making daily backup of small quantities of documents uneconomic.
- Specialized equipment is required to read it, which may not be immediately available after a disaster.
- Unit Record problem: An active file may end up on multiple reels.

Microfilming services, source documents filming, and output of electronic records to microfilm (COM), are available from the State Archives Imaging Services Program as well commercial providers. For further information on costs, contact your Regional Archivist.

The Washington State Archives provides security microfilm storage and inspection services at no cost to local agencies. For further information on costs, contact your Regional Archivist.

Electronic Imaging

This is an increasingly viable solution for protecting essential records. Imaged records are replacing both paper and microfilm as active records in offices.

Advantages:

- Imaged records can be inexpensively written to CDs, tapes or other electronic media.
- Electronic images can be "shipped" and stored at low cost.
- The original paper records can be sent to storage and serve as security for the imaged record.
- Electronic images of documents of reports can be output to microfilm as a fail-safe backup.
- No unit record problem.

Disadvantages:

- More expensive that microfilm.
- May require expensive indexing.
- Data on backup CDs or tapes must be redone each time software or platforms are upgraded or replaced. Electronic information in outdated formats cannot be read by current systems.
- Avoid proprietary systems, closed system architecture, non-standard file formats and compressions, which inhibit your ability to migrate essential records information to new systems.

Commercial imaging service providers are located in most major Washington State cities. Contact your Regional Archivist for further information on requirements for electronic imaging systems.

See the Chapter 3 and Appendix B-4 for protecting electronic records.

STEP 3 - DEVELOPING AN ESSENTIAL RECORDS SCHEDULE

Once the essential records are identified and methods of protection are decided they should be documented in an Essential Records Protection Schedule.

An Essential Records Schedule will identify:

- Records series that require protection.
- The office of record which has responsibility for it.
- The media on which it is captured.
- Instructions for protecting it, including the method of duplication, if appropriate, and the storage location.
- The frequency it is to be updated.
- Its total retention as a security copy.

Develop an Essential Records Protection Schedule by:

- Using "Essential Records Protection Schedule" (Form SAA-38) in Template A-2.
- Adding a "Protection Instruction" column to an existing agency or office retention schedule.
- Using a spreadsheet or table.

Figure 1: Example of an Essential Records Schedule

STEP 4 - IMPLEMENTING AN ESSENTIAL RECORDS PROTECTION PLAN

The Essential Records Protection Schedule and Plan should be implemented by each agency office in accord with the update cycle for each record series. This may mean weekly, monthly or perhaps only annual duplication or replication and off-site storage of some essential records. Obviously, the more frequent the implementation, the better the protection.

Protection of other essential records may require no action at all, because the method is simply their continued storage in secure on-site cabinets, vaults or record rooms or because they are automatically protected by natural dispersal.

AGENCY NAME: Central City					SCHEDULE DATE
No.	**SERIES TITLE**	**OFFICE**	**MEDIA**	**UPDATE CYCLE OR TOTAL RETENTION**	**PROTECTION INSTRUCTIONS**
1	Accounts Receivable	Finance	Paper	Daily	Scan. Back up images to DAT tape. Store tapes off-site
2	Accounts Payable	Finance	Paper	Daily	Scan. Back up images to DAT tape. Store tapes off-site
3	Payroll Reports	Finance	Electronic (Payroll System)	Monthly	Computer Output Microfilm (COM). Store security copy at State Regional Archives
4	Critical Materials List	Public Works	Paper	Monthly	Microfilm. Security copy at State Archives

Note: Development of an essential records protection plan should be done through a formal POLICY and PROCEDURE approved by agency management. A model policy and procedure is found in Appendix A-1.

STEP 5 - TESTING THE SYSTEM

Test the effectiveness of the Essential Records Protection system annually. This can be done by checking to see that:

- On-site facilities are secure.
- Essential records are stored properly.
- Security copies exist.
- Security copies stored off-site.
- Security copies are updated according to the schedule.
- Security copies held by other offices still exist.

CHAPTER 2: RECORDS MANAGEMENT

A. The purpose of records management program is to minimize the physical volume of an agency's records, streamline records retrieval, improve the integrity of files, reduce risk, and cut costs. It is much easier to protect essential records if a proper records management program is in place.

B. Good records management practices facilitate disaster prevention and disaster response for the following reasons:

- The organization will know what records it has, where they are located, and who is responsible for them.
- Records management information is necessary for prioritizing resources for essential records protection, as well as recovery and replacement of damaged records.
- Restoring records costs money. For example, some recovery methods can cost as much as $250 per box. Without a records management program it may not be possible to separate damaged records that your agency needs to restore or replace from those that it doesn't. This can result in restoring more records than necessary, a waste of time and money.

- If records retention schedules are properly followed, inactive and obsolete records are already removed from the office. They will not need to be dealt with during an on-site disaster or emergency. This saves time, money and reduces risk.
- During the recovery phase, records that have been salvaged must be returned to their rightful place. A records program provides the information necessary to determine where the right place is.

C. FOR FURTHER INFORMATION ON DEVELOPING AN EFFECTIVE RECORDS MANAGEMENT SYSTEM, CONTACT YOUR REGIONAL ARCHIVIST.

CHAPTER 3: ELECTRONIC RECORDS

A. Background: Electronic records are steadily supplementing or replacing conventional records in most organizations including local governments. Electronic records are often easier to protect than paper records because backup can be automated, backup storage is inexpensive, requires little physical space, and large amounts of data can be moved more easily in electronic format than hard copy.

Electronic records are legally no different than records stored on conventional media such as paper or microfilm. However, in practice, there can be large differences in the way electronic and conventional records are managed and protected. For example, electronic records must be protected at the beginning of the information life cycle by back up and duplication. Trying to rescue damaged tapes and disks is often impossible and should be considered a last resort.

A major difference between electronic and conventional records is the expected speed of recovery. Extensive damage to a paper-based system may require weeks or months for full recovery, yet be considered a successful recovery, whereas a one week recovery of an electronic system may be considered unacceptably slow.

Electronic systems are usually supported by technical infrastructures including mainframes or servers, local area networks, PCs, operating systems, database management systems, and the Web. An agency will usually have a relatively small number of large, centrally managed systems, with perhaps a larger number of smaller systems on workgroup level servers or individual PCs. The large systems are usually managed by an Information Technology (IT) organization, but management of small systems may be decentralized even to the individual worker.

B. Disaster Prevention for Electronic Systems: Prevention begins with system design. Fault Tolerance, also called redundancy, helps to provide protection not only against data loss but also against down time caused by system failures. Generally, the more that fault tolerance is built in, the more expensive the system (See Appendix B-4).

- An example of fault tolerance is the use of RAID (redundant array of inexpensive disks) for data storage. With RAID no single disk drive failure will result in data loss or down time.
- Another example is the use of UPS (uninterruptible power supply) to make sure systems shut down gracefully when there is a power outage.

C. Protection Methods: The basic method of protecting electronic records, like paper records, is duplication, with the duplicated data stored off-site. Five alternative methods of data backup and duplication are summarized below. The first is the cheapest and most basic. Succeeding methods are progressively more expensive, but faster and more comprehensive. (See Appendix B-4.)

Keeping backups beside the computer defeats the purpose.

1. **Backup and Restore:** Backup data from magnetic, optical or other storage media are routinely copied to disks or tapes and stored off-site. If working data is lost or damaged, the backup data can be retrieved and restored to the system. In addition to data, it may be necessary to reinstall the operating systems and application software, therefore system tapes and/or disks and written documentation must be stored off site but available to the disaster team. The backup and restore concept applies to systems of all sizes.

   Imaging systems often back up optical disks by writing the data to two optical disks simultaneously. The back-up or mirrored disk is stored off site.

   Data may also be sent electronically to an off-site backup server, eliminating the need to create backup tapes or disks and physically move them back and forth.

2. **Cold Sites:** A cold site is a place that is ready for installation of servers and other hardware. In case a data processing site is destroyed or rendered temporarily unavailable, the computer hardware may have to be replaced before data backups can be restored. A cold site has raised floor, power supplies, communications, and air conditioning but does not have pre-installed computer hardware.

3. **Hot Sites:** A hot site, like a cold site, is a remote facility used to restore electronic operations when a disaster has rendered normal facilities and/or hardware inoperable. Computer hardware is already installed and is ready for uploading systems and data.

4. **Near Line:** A near-line facility is a version of a hot site in which periodic (usually nightly) backups of information are sent electronically. The near-line hardware is continually updated. In case of a disaster to the normal facility, the near-line facility can take over almost immediately and will be as current as the latest backup. This avoids the need to send system and data tapes to the site and eliminates the time required to bring up the system.

5. **On line Mirror Site:** Real time duplicates of essential files are maintained at the site. Fast communication links enable data to be written simultaneously to both the normal site and the on-line remote backup site. In case the normal site is disabled, the mirror site takes over immediately with virtually no down time. This alternative provides the fastest recovery but is usually the most expensive.

Backup Services:

Alternative 1, backup and restore, is usually carried out by the agency itself.

Alternatives 2 – 5 usually apply to larger systems. Because of expense, only larger organizations can afford to build such backup sites themselves. These services are often provided by commercial firms under contract. The sites may be long distances away.

An emerging option is to have a local government build these capabilities for itself but with extra capacity so as to be able provide these services to other governmental organizations.

> For example, Yakima County has a backup facility able to provide all the above services (1-5) to other state and local governments under

inter-local agreements. This can provide excellent backup and duplication services even to small governments at a more reasonable cost than previously available.

D. Other Duplication Methods:

Computer Output Microfilm (COM): This is a form of duplication in which reports from computer systems including mainframes are automatically indexed and output directly to microfilm. It is also used for images or other electronic documents. COM is not intended for databases or multimedia. The microfilm can be stored off site and retrieved in case of disaster. The Washington State Archives provides a COM service for TIFF Images, MS Word, Excel, PDF, and other files to state and local agencies as well as storage services for the security microfilm.

Computer Output to Laser Disk (COLD): This is similar to COM except that reports are written to removable media such as CDs instead of microfilm. The removable media is stored off-site. The process is also known as Enterprise Reports Management (ERM). COLD CDs need to be rewritten as the software applications that are used to access records data are upgraded or changed.

Source Documents: Another form of duplication is to maintain the paper source documents and to re-key the data if the data is lost. This is time consuming and expensive.

Email: The IT department will usually back up email documents. Email messages that contain public record information should be moved into the agency's records keeping system as soon as possible and filed with the appropriate records series.

Key Essential Records Protection Issues:

1. Is there a centralized IT department? If not, the records officer may need to become actively involved in advocating the developing of a disaster plan for electronic records.

2. If there is a central IT department, does it have a Disaster Plan or at least backup procedures? If not, a regular backup process and Disaster Recovery Plan should be developed for the IT system as soon as possible.

3. If there is an IT disaster plan or backup procedure, does it cover essential electronic records? If not, the plan must be modified to include them.

4. Does the IT disaster plan or backup routine cover smaller group level servers and systems, PC based systems, laptops, and disks? If not, they should be.

E. Workgroup Level: Some smaller systems are not supported by centralized IT operations. Records may be stored on Local Area Network (LAN) servers, PC hard drives, removable magnetic disks or tapes, Compact Disks (CDs) or floppy disks. Disaster planning and recovery procedures should be written for small systems not supported by a centralized IT organization or by a LAN manager.

The most effective strategy for protecting data on small systems is to duplicate it and store the backup duplicate off-site. It is much more efficient to recover lost data from an off-site backup than to try to salvage magnetic tapes and disks after they are damaged. See Appendix C-9 for information on restoring magnetic or optical media.

- Backup PC and laptop data to the LAN, if the LAN itself is regularly backed up.
- If not backed up to the LAN, PCs and laptops should be backed up routinely, normally daily and weekly onto removable media for off-site storage.

- Written documentation and procedures for backup and recovery must also be stored at the off-site location. The PC user may not be around during or after a disaster, and someone else may have to restore the data.

A disaster could render the PCs or other hardware inoperable and the office space they occupy unavailable. Therefore the disaster plan should provide for alternate sites and equipment. The disaster team must be able to restore operating systems, application programs, and data on entirely new PCs or similar computers.

See Appendix B-4 for additional information on backing up PCs.

CHAPTER 4: RISK ANALYSIS

Generally, there is not enough money or time to protect all records against all eventualities. There may not even be enough to protect all essential records. Risks need to be analyzed and priorities set for protecting individual records series. The most common methods are Functional Analysis and Physical Threat Assessment

A. FUNCTIONAL ANALYSIS: This is a simple tool for assessing risks and setting priorities. The tool works for both conventional and electronic records. Each line represents a function. The function may generate one or more record series and/or information systems. Each department is asked to list its major functions. For each function, set a probability number between 0 and 5 (with 5 being the highest) representing the likelihood of a disaster or damage affecting these records.

For example, if the records are located in the basement in a flood plain area, the number might be set at five. If they are located in the Police Department in a secure, fire protected location, with a backed up data system, the number might be set at 1. The second number is the Consequences Number. Higher numbers indicate greater estimated adverse affects on continuity of operations. The product of these two numbers is the Risk Number, the higher the number, the greater the risk.

RISK ASSESSMENT				
NO.	**NAME OF FUNCTION**	**PROBABILITY OF DISASTER 0 - 5**	**CONSEQUENCES OF DISASTER 0 - 5**	**RISK NUMBER 0 - 25**
1	Accounts Payable	3	5	15
2	Payroll Records	4	5	20
3	Police Incident Reports	1	5	5
4	General Correspondence	4	2	8
5	Working Files	5	1	5

Figure 2: Risk Assessment Example.

Payroll and accounts payable records have the highest risk numbers and should receive protection priority. Police reports, while just as valuable, have a low risk number because of the low probability number.

This should be taken into account when developing an essential records program and when writing a Disaster Recovery Plan. For example, both payroll and police incident reports are normally considered essential records. But in this example, there may be only enough funds to duplicate one set. The risk number would indicate that that payroll records should be duplicated first.

All facilities are vulnerable to fire, routine water damage, and mold. In addition, are severe storms or earthquakes a danger in your area? Consider the location of your building(s) and nearby flood plains, rivers or creeks, railroad tracks, airport flight paths, or a nuclear power station. These will suggest the scope and type of disasters for which you should plan.

B. PHYSICAL THREAT ASSESSMENT: A key component of disaster prevention is awareness and correction of weaknesses in agency facilities and buildings that could cause a disaster, or exacerbate one resulting from another cause.

For example, un-braced shelving can topple over during an earthquake and spill boxes of records onto the floor (a mess but not a disaster). However, if the quake causes pipes to burst, the records thrown to the floor may be soaked, resulting in a disaster. If the shelving is braced, it probably will withstand the quake, and even if pipes burst, chances are only the bottom shelf of boxes will get wet.

The Physical Plant Threat Assessment can spot weaknesses within agency facilities that may result in a disaster that affect records or exacerbate damage from another cause.

Threat Assessment Inspection Checklists: Simple checklists can be used to identify, correct physical threats. Each checklist should identify a subject of inspection such as fire protection, files and records storage areas, plumbing and water, and specific points to be inspected. It should also identify results of the inspection and actions taken.

Inspections may be done by facilities maintenance, safety and fire prevention personnel. Such inspections should be done on a regular annual basis. Create a procedure for gathering information from annual inspections and confirming that remedial actions are completed.

Files and Record Storage Areas	**OK?**	**Needs Action** (Describe)	**Action Complete** (Date & Initial)
Shelves well-braced	No	No existing bracing and shelving is not bolted to the floor.	Braced & bolted by Maintenance 2/11/03
Items shelved snugly			
Shelving 4-6" off floor			
No materials stored on floor			
No essential records or valuable materials in basement			
Exits unobstructed			
Important materials away from windows			

Figure 3: Checklist Example

The records disaster recovery team should inspect record-storage areas to identify conditions that could trigger or aggravate damage to record information. Some items will need attention only once (for example, correcting unsatisfactory shelf bracing). Other items require periodic inspections, such as furnaces and boilers. Some conditions will be found that require repair, replacement, or other maintenance activity. For example, if drains are not flowing freely, a simple cleaning could remedy that condition. If fire extinguishers are missing from a critical area, they should be purchased and installed. Other conditions may not be so easily remedied due to cost. For example, if there is no automatic fire suppression system, it may not be possible to immediately install such a system. However, the resultant vulnerability should be identified and funds requested in the agency budget.

Physical Threat Inspection Checklist Templates   Appendix B - 7 contains a set of checklist templates covering other areas of specific concern to records disaster prevention. These templates are also on the accompanying CD and the Secretary of State's website. Their use can reduce records damage vulnerability.
The first section of the appendix, "Records Disaster Risk Assessment and Prevention Procedures," is a fill-in template that can be used to document responsibility, schedule inspections and indicate distribution. Forward copies of the completed inspection report to risk management.

SUMMARY: Once the risk analysis has been done, essential records identified and protected, physical threats documented, removed or reduced, the prevention phase will be complete. This will result in:

- Protecting the most important records.
- Lessening the damage that can be caused by a disaster.
- Identifying those records that merit recovery if they are damaged.

Prevention procedures should be reviewed and updated each year.

PART II: PREPAREDNESS

This part of the Records Disaster and Recovery Manual covers the Disaster Preparedness and Recovery Plan. Chapter 1 outlines the purpose and function of the plan. Chapter 2 shows how to write the plan. Chapter 3 covers testing the plan. There are several associated appendices that contain detailed procedures and fill-in templates for developing a records disaster plan.

CHAPTER 1: THE RECORDS DISASTER PREVENTION AND RECOVERY PLAN

A. DEFINITION AND PURPOSE

The Records Disaster Prevention and Recovery Plan (RDRP) is a customized plan, written by those responsible for an agency's records, approved and published by management, that contains actions that should be taken to reduce the risk of disaster, and to respond and recover from disasters that do occur.

A plan will not succeed without management support. Top management, by approving and endorsing the plan, will add force to the program.

B. BENEFITS

The benefits of prevention and preparation were covered in Part I. The benefits of a plan during and after a disaster are:

- Speed: Fast action is critical to responding to a records disaster. A plan already in place enables rapid response.

- Correct decisions: Actions taken must be the correct actions. A plan in place ensures that the people making the decisions are the people who know what to do.

- Coordinated action: A plan minimizes the tendency of various staff members and managers to make individual decisions about records. Individual decisions made during crisis situations may not be correct.

- Delegated authority: Policy, authority, and responsible delegations should be established before a disaster occurs. Sometimes people do not want to be responsible for dealing with damaged records. Sometimes too many people want to be responsible.

- Designated records team: The plan defines the roles of the team and team leader.

- Targeted resources: This includes funding authority, work areas, relocation sites, supplies, and contracts or relationships with outside vendors who may be needed.

- Established communications: Methods of communication are in place.

If a records disaster plan does not exist before a disaster occurs, it will have to be put together during the disaster. This is not easy to do in the dark, ankle deep in water, often on a weekend or holiday.

Ideally all the players who must take part in response and recovery from disasters will have participated in developing and approving the plan.

C. WHERE DOES THE RECORDS DISASTER PLAN FIT INTO THE FAMILY OF PLANS?

A records disaster plan does not exist in a vacuum. Other disaster plans may already exist. For example, local governments usually have general disaster plans that cover such things as evacuations, building security, fire prevention and bomb threats. Often these plans are based on Emergency Management Division (EMD) templates.

It is not necessary or desirable that the RDRP duplicate or conflict with provisions of the general disaster plan. But the RDRP probably will have features not found in the general plan. It is possible to embed the RDRP in the general plan, but it will probably be too large to be accepted. A good way to relate the two plans is to have the general plan refer to the RDRP by reference and policy. Records team members should be familiar with the basic features and procedures of the agency plan.

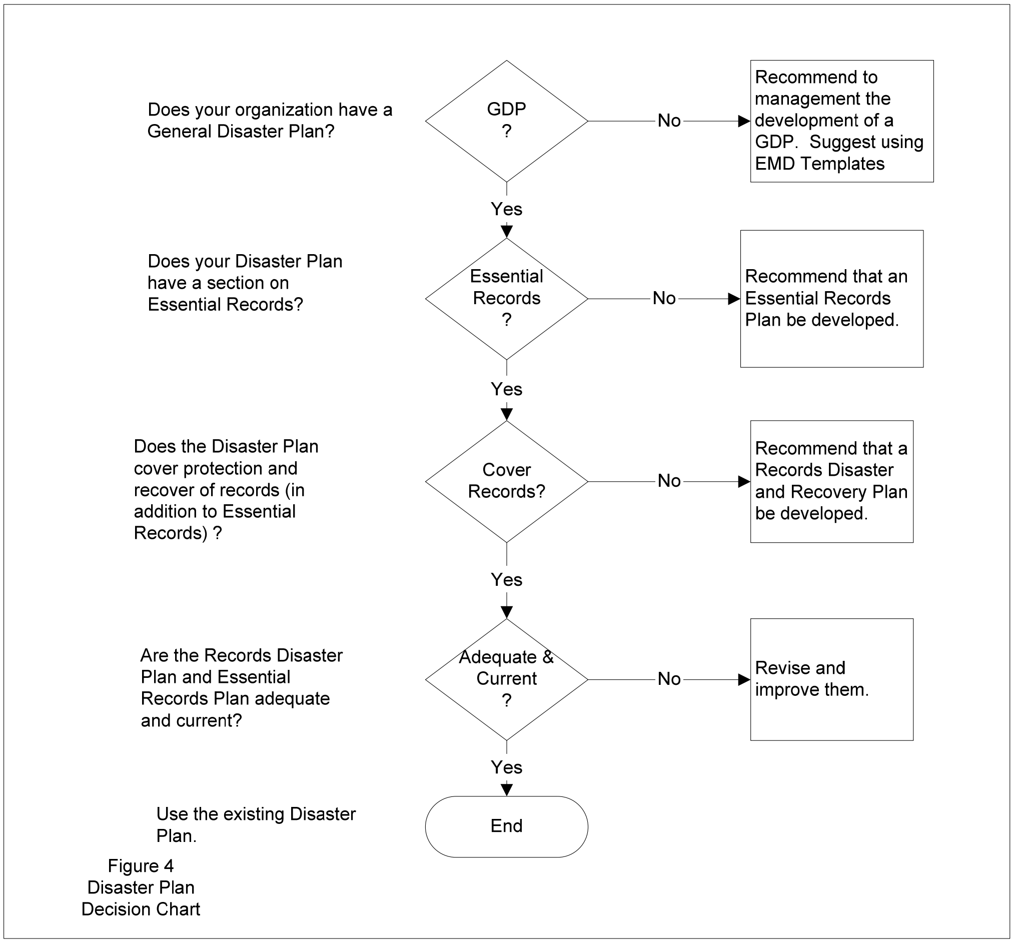

Does your organization have a General Disaster Plan?
GDP ?
No
Recommend to management the development of a GDP. Suggest using EMD Templates
Yes
Does your Disaster Plan have a section on Essential Records?
Essential Records ?
No
Recommend that an Essential Records Plan be developed.
Yes
Does the Disaster Plan cover protection and recover of records (in addition to Essential Records) ?
Cover Records?
No
Recommend that a Records Disaster and Recovery Plan be developed.
Yes
Are the Records Disaster Plan and Essential Records Plan adequate and current?
Adequate & Current ?
No
Revise and improve them.
Yes
Use the existing Disaster Plan.
End
Figure 4
Disaster Plan
Decision Chart

Figure 4: Disaster Plan Decision Chart

Similarly, if a local government has an Information Technology (IT) Department, that department may have a disaster plan or at least a back up and restoration procedure. If the plan or procedure is adequate, it should not be necessary to duplicate it. If not, the RDRP may have to address electronic records. (See Part I, Chapter 3, Electronic Records and Appendix B-4.)

CHAPTER 2: WRITING THE RECORDS DISASTER AND RECOVERY PLAN (RDRD)

The main components of most Records Disaster Plans are:

A. Management Approval and Support - Policy
B. Authority and Responsibility – Records Disaster Coordinator
C. Records Preparedness and Response Team
D. Training and Provisioning the Team
E. Support
F. Communications
G. Essential Records Protection Procedure Section
H. Preparedness and Prevention Procedure Section
I. Response and Recovery Procedure Section
J. Appendixes and Glossaries as needed

Use the attached templates in Appendix A, B, C and D to help write the plan. Begin with the Policy Statement in Appendix A-1, continue with the cover sheet (Distribution List), Appendix B-3, etc, using templates as noted.

See Part III for executing the plan and for making tactical decisions based on actual circumstances (after a disaster).

A. MANAGEMENT APPROVAL AND SUPPORT - POLICY

Approval and support are expressed initially by a policy statement signed by a senior management official or officials. This should be one of the first pages of the plan. The policy statement should include delegations of authority for decision making during and after a disaster. It is important that the lines of authority be determined in advance. Authority to commit funds and contract for services should be included. See Appendix B-1 for a policy statement template.

B. AUTHORITY AND RESPONSIBILITY - RECORDS DISASTER RECOVERY COORDINATOR: One person must be assigned the full authority and responsibility for response to and recovery of agency records after a disaster, large or small. This person would also direct the records disaster team. For purposes of this manual we are using the title Records Disaster Coordinator (RDC).

The RDC oversees the details of the recovery in consultation with the agency head, director, or other administrators. He or she reports directly to chief agency administrator, city manager, mayor, county, or district administrator and:

- Works within the agency's Emergency Management Plan and with members of the agency emergency management committee, agency risk management, purchasing, personnel, and maintenance offices;
- Develops an agency records disaster prevention, response and recovery plan in consultation with a records disaster recovery team and agency emergency management officer and/or committee;
- Develops and implements the agency essential records protection plan and schedule;
- Develops and implements a records disaster preparedness and prevention procedure;
- Directs all response and recovery operations involving records;
- Supervises the packing and transportation of records, drying and other recovery activities, storage arrangements, documentation of movement and treatment, and long-term restoration and rehabilitation of records;
- Assigns some functions to departmental records disaster coordinators, including supervision of work recovery crews.

These duty statements can be written into the plan.

C. BUILDING A RECORDS PREPAREDENESS AND RESPONSE TEAM

This section is intended to help build a successful team approach to help plan, prepare, and recover from a disaster that affects records in the agency or organization. See Appendix A-4 for an appropriate template.

The team should consist of departmental records disaster coordinators: These are designated individuals from each of the departments or subdivisions of the agency who are knowledgeable about their department's records. Department coordinators should be appointed by the department director and have that director's support. They should have authority and responsibility for protection, preparedness, response, and recovery actions under the overall supervision of the agency RDC. Often, if an agency has a records management program, departments will have records coordinators assigned to work with a records manager. These same people might best serve on the records disaster team.

The disaster preparedness and response team has four primary responsibilities:

1. Assist and advise the records disaster coordinator in developing and selling the Records Disaster Recovery Plan to management. A team approach to forwarding and gaining management support is usually superior than going it alone.

2. Assist in developing and implementing the essential records protection schedule and plan.

3. Engage in and support response to and recovery from a disaster. A records disaster of even small proportions stands a better chance of successful recovery through teamwork.

4. Supervise response and recovery at the departmental level; provide guidance on recovery priorities, disposition decisions, and replacement options for records.

These duties can be written into the plan.

D. TRAINING AND PROVISIONING THE TEAM

Emergency Response Information Packet: Each member should be supplied with an Emergency Response Information Packet, to be kept at home or in the car and brought to the disaster site in the event of an emergency. The packets should include the following materials. (Some or all of these items may be included within each team member's copy of the disaster response and recovery plan.)

- A list of the names and phone numbers of the DPT members
- A copy of the "Emergency Response and Salvage Wheel" by the National Task Force on Emergency Response
- A copy of the agency's records retention schedule and essential records retention schedule
- A diagram of each floor designating location of essential and other records
- A list of resource people (conservators, archivists, and other professional advisers) and their phone numbers
- A list of volunteers and their phone numbers
- A copy of the agreements with vendors relating to emergency response services such as cold storage
- A copy of the forms and instructions to be used during recovery procedures, such as initial damage appraisal, damage location inventory, and removal inventory
- Keys and combinations to records storage areas

Relevant templates are found in Appendices A-E.

Training: Members of the disaster team should be provided with training to enable them to carry out their responsibilities in a disaster response and recovery operation. This may range from annual, full-scale disaster simulation drills to periodic workshops. At a minimum, plans must be made for on-the-spot training in the event of a disaster. Training should be documented in the plan for budget purposes.

Personal Equipment: The agency should provide rubber pull-over boots, hard hats, disposable rubber gloves, and particulate filtering face masks for recovery team members and work crews. In addition, members of the disaster team should assemble and maintain their own personal kit containing clothing, and personal items such as medications, if any, that they will need during the first eighteen hours of a disaster recovery operation.

E. SUPPORT

The Essential Records Protection and Disaster Recovery Plan needs to adapt to and be supported by the agency emergency management plan. It may also need the support of other offices within the agency. The following functions are crucial to a successful disaster preparedness and recovery plan.

- Facilities management and maintenance: Responsible for facility maintenance, repair and inspection essential to records disaster preparedness. Manages clean-up and repair of physical plant after a disaster.

- Finance: Approves expenditures for emergency supplies, equipment, and services such as cold storage.

- Information systems: Manages mainframes, servers, Local Area Networks, and PCs. Manages operating systems, applications programs, email, and Web portals. Oversees system backups, provides for backup storage, and manages relocation of electronic information equipment and records to secure off-site facilities after a disaster. Manages or contracts for recovery of electronic information hardware, software and data.

- Purchasing: Acquires recovery supplies, locates emergency space and services for drying, storing, shipping, freezing, and freeze-drying damaged records.

- Risk management: Documents losses, notifies and negotiates with insurance companies and FEMA.

- Safety and health: May authorize evacuation and re-entry into the disaster site.

- Security: Local police, sheriff, or agency security officer will secure the grounds and facilities and control access after a major disaster.

The records disaster coordinator should provide managers in each of these areas with copies of the Records Disaster Recovery and Essential Records Protection Plans and work with managers to insure the flow of materials, labor and services needed for response to and recovery of disaster damaged records.

- Fire Department: It is the fire department that decides when a fire-damaged structure can be re-entered. Since time is of the essence in records recovery, the fire department and the disaster recovery team need to develop a good working relationship. The urgency of early access to wet records and the need to avoid “collateral damage” to records during fire suppression should be emphasized. Teams should provide the fire department with floor plans designating the location of essential records. If the fire department can enter and suppress the fire from within the building, and can locate the essential records, it can often limit water damage.

Coordination with providers of other related functions should also be written into the plan.

- Consultants: Consultants are sometimes needed to provide the agency with temporary specialized support. These might include: records management and information systems consultants, FEMA and EMD consultants, State Archives and other outside organizations that might provide support and resources.

- Conservators: If your agency has valuable records on specialized media, such as blueprints, sepias, coated papers, or photographs, you may want to consult a paper or photographic conservator during the planning and preparedness process, and have one on a "standby" agreement to assist in response and recovery.

- Recovery Specialists: Few commercial companies specialize in records recovery. Recovery specialists offer experience and expertise in recovering records from both large and smaller disasters. A short list of these companies is in Appendix C-5-4.

RECORDS DISASTER PREPAREDNESS AND RECOVERY PLAN

Placement, Team, and Support

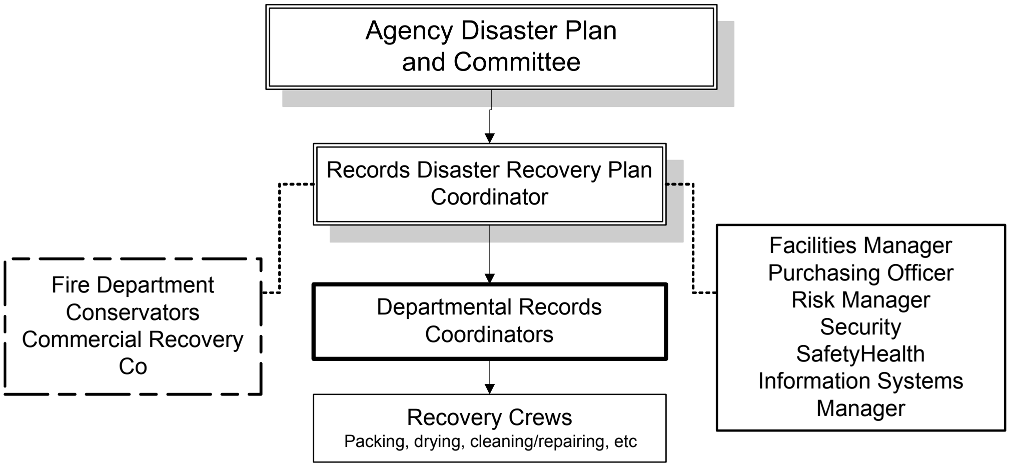

Agency Disaster Plan and Committee
Records Disaster Recovery Plan Coordinator
Fire Department
Conservators
Commercial Recovery Co
Departmental Records Coordinators
Recovery Crews
Packing, drying, cleaning/repairing, etc
Facilities Manager
Purchasing Officer
Risk Manager
Security
SafetyHealth
Information Systems Manager

Figure 5 Organization Chart

F. SIZE, COMPOSITION AND STRUCTURE

The makeup of a records disaster response and recovery team will depend on the size of each organization and the scope of each disaster. A minor emergency can be handled by a small group working together on a fairly informal basis. Larger disasters require more people as well as more formal organization and reporting lines.

When minor emergencies occur, most of the recovery functions can be handled by the records disaster recovery team and other agency staff. A large scale disaster, such as a major fire in a building, may require contracted experts to handle the entire recovery, or, at a minimum, volunteers and day labor.

G. COMMUNICATIONS

Communications cover the normal chain of command from senior executives, communication between the Disaster Coordinator and Departmental Coordinators as well as communication between team members. It also covers communication with outside sources of help such as FEMA and the Emergency Management Division (EMD). See Appendix A4-1 and A-10 for template lists of emergency telephone numbers. Such a list should be part of the plan.

H. ESSENTIAL RECORDS

See Part I, Chapter 1, and use the Essential Records Schedule Template in Appendix B-2 as well as the listing of Essential Records in Appendix B-3. When the Essential Records Plan is completed it should become part of the Records Disaster Recovery Plan (there is a place for essential records in the EMD template for agency overall disaster plans that may also be used).

I. PREPAREDNESS AND PREVENTION SECTION

Risk assessment information (see Part I) may be placed in this part of the plan. Appendix B-6, 7 may be used to document physical threats and other aspects of prevention. Use of these tools should be part of the procedures identified in the plan.

J. THE RESPONSE AND RECOVERY SECTION

NOTE: The plan described in this section is a generalized or strategic plan with probable response and recovery procedures. Actual procedures used and choices of alternative courses of action (tactical decisions) will depend on circumstances. See Part III for choosing between alternative response and recovery procedures, and for appendix and template references.

Procedures for recovering records from a disaster should be part of the Records Disaster Plan, however separate hands-on information for recovery can supplement the plan along with response procedures. This will help ensure that all additions and updates to the section are properly distributed. Remember also to update the master and backup copies of the plan.

Your Records Disaster Plan should include procedures for the following basic response actions:

- Gaining access to the facility as quickly as possible.
- Making an initial assessment of damage to any records.
- Reporting findings to the agency disaster management officer or, if no agency-wide plan exists, to the chief administrator. (See Appendix C for Initial Records Damage Assessment Report template.)
- Assembling the record disaster response team using the emergency call list or telephone tree.
- Briefing the team on the nature and extent of the damage.
- Assigning team member tasks:
  - Stabilize the environment.
  - Locate and set up a response and recovery operations center.
  - Identify, locate and acquire needed supplies.
  - Prepare detailed damage assessments.
  - Perform triage – treatment decisions based on previously established recovery priorities and detailed damage assessments.
  - Remove and dispose of obsolete records and records that are damaged beyond recovery.
  - “Pack-out” records destined for temporary cold storage and/or freeze or vacuum drying.
  - Transfer records to an on-site or off-site location to be cleaned, air dried, interleaved and/or copied.

Track each action by box or record, indicate what it is, and where it is going i.e. disposal, salvage cold storage, freeze drying, etc., using either an automated or paper tracking system developed as part of the planning process.

The disaster response part of your plan should include procedures for implementing each of these actions. Appendix C includes procedural templates and instructions for response and recovery actions.

A general plan of operations must be established before any recovery activities are started. The volume of materials involved may be the determining factor in deciding which recovery procedure to implement.

The following recovery procedure questions should be addressed in the process of developing records recovery plans:

- How will the steps be carried out?
- Who will be responsible for each?
- Who will supervise?
- Where will the work be done?
- What kind of workflow makes sense?
- Who has authority to authorize disposal of items that are unrecoverable?
- What funds are available from the operating budget and/or from insurance coverage?
- What rehabilitation priorities must be set so that essential services are quickly restored?
- What activities may be done in house by the staff, and when should services be contracted?

CHAPTER 3: TESTING THE PLAN

No plan can be effective unless it is tested regularly. This is especially true of plans for electronic records but applies to all records. It is vitally important to test the communications areas of the plan including the ability to assemble a disaster team quickly.

Desktop test: A desktop test is a small scale test involving only the core team members including the records disaster coordinator, the disaster team, one or more departmental records coordinators, and key staff members such as facilities, IT director, etc.

- Write a scenario. (Water damage from burst pipe, etc.)
- Test communications. Call relevant team members and staff.
- Assemble the disaster team.
- Assess damage.
- Plan appropriate response.
- Evaluate results.

Larger scale test: This is a fully developed test involving more people and simulated records damage. An auditor might be invited to observe the test and help evaluate the results.

- Write scenario. Provide copy to Auditor in advance.
- Identify and flag "damaged" records in advance.
- Test communications. Call team members, operational staff, and fire department, etc.
- Assemble team(s).
- Test operations center.
- Detailed assessment of damage.
- Possibly test IT restore procedures.
- Plan appropriate response(s).
- Move records to simulated storage and repair area.
- Test documentation procedure.
- Test availability of supplies.
- Return and re-shelve "restored records."
- Evaluate results.

Testing of information systems supported by IT staff is a specialized process requiring a technical background. Testing backup and recovery of PCs and laptops requires less technical expertise. PC and laptop owners should be able to test backup and restore procedures.

PART III -- DISASTER RESPONSE AND RECOVERY

Disaster response is defined as assessing damage and taking actions that will minimize additional damage and permit the most effective recovery of records or information. Both strategic and tactical responses are needed when facing a records disaster.

CHAPTER 1: RESPONDING TO RECORDS DISASTERS

A. STRATEGIC RESPONSE:

The Records Disaster Plan described in Part II is a strategic plan designed to provide a basis for responding to any kind of disaster. (Specific responses to actual situations will vary and are covered under tactical response, below). Initial response for any disaster is likely to include the following basic steps:

- Gain access to the damage site. It is essential to gain access to the damage site as quickly as possible because some records will begin to deteriorate within 12 hours and mold will begin to grow within 48 to 72 hours. Access will be decided by the fire department, safety officer or another authority and can be delayed for days or weeks, pushing the envelope for recovery.

Six Keys to
Successful Response and Recovery

1. A detailed Disaster Recovery Plan
2. Committed management
3. Educated and trained staff
4. Timely initial response
5. Effective communication
6. Quick, informed decisions

- Assemble the recovery team. Using pre-arranged communication links, bring in the recovery team as quickly as possible to help control the situation and carry out other response steps. (See Appendix A-4-1.)

- Establish controls. Set up a recovery command desk from which all actions regarding all records in the damage area must be cleared. Insist agency policy and procedure regarding the handling of all records be followed after a disaster. Experience shows that often agency staff will attempt to take matters into their own hands, resulting in further damage and loss of records and the intellectual control over them (what records existed, where, extent of damage and what happened to them, information essential for insurance and disclosure purposes). If necessary, assign recovery team members the task of enforcing agency disaster recovery policy and securing records from uncontrolled and untrained efforts to “clean house” or recover records. (See Appendix C-3-2.)

- Make an initial damage assessment. Using recovery team members, make a quick “walk through” of the damage site, noting the general volume of records damaged and undamaged, extent and type of damage, i.e., water, fire, contamination, or a combination such as edge damage, charred and wet, or mostly burnt and saturated. Photograph the damage with either a digital or Polaroid camera. This will provide information necessary for insurance or audit purposes. (See Appendix A-6.)

- Establish communications. Prepare initial report to management. Notify agency staff, outside support agencies and, if appropriate, give advance warning to conservators or commercial firms that may be needed in the recovery effort. Contact your Regional Archivist. (See Appendix A-8 and 9.)

B. TACTICAL RESPONSE:

Tactical responses are situation specific. They include actions that may be anticipated in the "Strategic Plan," but which can only be decided based on the nature and extent of the disaster.

- Decide on method of stabilizing the environment and records, based on damage assessment;
- Re-assign recovery priorities, if necessary, based on level of damage and "recoverability;"
- Decide on methods of drying and recovery;
- Assemble supplies, equipment, additional personnel or contracted services.

The initial reaction of people undergoing a disaster is often shock and disbelief. People are more concerned with where they will work tomorrow or how they will be paid than in dealing with damaged records. Records often have a low emotional priority, but they have a high real priority in terms of continuity of operations. It is the task of the records coordinator and the team to focus agency and staff attention on the records. This must be done immediately. The "need for speed" is paramount in responding to disasters.

Decide on the method of stabilizing the environment and records, based on damage assessment.

The disaster coordinator and team will need to make response decisions based on the nature and scope of the disaster and resources available. Much of this will be determined by circumstances. The following **must be known in order to make fast, accurate decisions:**

1. Is the damage to records large or small? If the amount of damaged records is small, agency staff should be able to handle it. If large, it may be necessary to call in outside resources such as document conservators, temporary help, and professional disaster recovery firms.
2. Is the damage to the facility minor or major? If minor, agency staff may be able to handle the problem. If major, the facilities or offices may need to be extensively repaired. If so, all records may have to be removed, damaged or not, before reconstruction can proceed.
3. Can the environment be stabilized? How long will it take?
4. What kind of damage? Most damage involves water. Other damage can involve fire, smoke, and contamination.
5. What kind of records? Do they include essential records or other important and non-duplicated records?
6. What kinds of media are involved?
7. What alternatives are available for drying and repair?
8. What funding is available?

(See Appendix A-6 for Detailed Damage Assessment Form.)

Stabilize the environment:

Structural stability: If the environment is rendered unsound by earthquake or other damage, can it be stabilized and returned to use rapidly? Work with facilities staff and appropriate government authorities to determine this.

Humidity: Continued high humidity will exacerbate existing damage to records, and facilitate mold growth on undamaged records. Reducing humidity will retard water damage and mold growth. Work with the facilities staff to see if HVAC systems can be restored. Humidity in small areas can be reduced by drawing in and circulating outside air. Humidity in large amounts may require the services of commercial de-humidifying firms. If humidity cannot be controlled rapidly, it may be necessary to remove all records. (See Appendix C-3-3, and 4.)

Re-assign recovery priorities, if necessary, based on level of damage and "recoverability."

The functional analysis described in Part 1 resulted in a priority listing for records protection, especially essential records. This prioritization may or may not be useful for records removal and recovery in connection with a specific disaster. Recovery decisions may have to be modified as a result of the nature and extent of the damage.

Disaster circumstances may force **a re-prioritization** of what records to salvage and in what order. Use the concept of "Triage" (a system of allocation of resources) to re-prioritize what records to salvage. Consider at least these three factors: (1) damage impact (2) value of the records and (3) extent of the damage.

(1) Damage impact:

> The extent of damage to records may make some media or records unrecoverable. High priority records simply may not be salvageable. The length of exposure to water, heat, chemicals, hazardous materials, or other adverse conditions reduce the chances of successfully recovery. For example, materials on coated paper may not be recoverable unless the recovery begins within about 12 hours. They may have to be abandoned in order to save other materials. In case of fire, plastic-based media (photographic negatives, microfilm and motion picture film, audio and videotapes) are easily damaged beyond recovery.

(2) Value of the records. Consider such factors as:

- High priority: Essential records or other records, especially those needed immediately.
- Medium priority: Records that have value but are not immediately needed.
- Low priority: Records that are obsolete, duplicated elsewhere, or unnecessary.

(3) Extent of the damage. Suggested priorities:

- First: Medium damage. Needs earliest treatment.
- Second: Minor damage. These records can wait a bit longer.
- Third: Extensive damage. Chances of salvage are low and costly.

The results of the "walk through" damage assessment and re-prioritization triage are part of the information needed to proceed. Further factors discussed in the following paragraphs must also be evaluated before making final decisions. (See Appendix C-3-7.)

C: STABILIZE RECORDS:

The first decision is whether and how to stabilize the records and avert further damage.

> Notes:
>
> 1. Do not move records without an inventory of what they are, to whom they belong, and where they are to be returned. (See Chapter II, Recovery - Information Management System.)
>
> 2. Avoid moving and storing valueless records as much as possible.

Options include:

- Freezing water-damaged records using cold storage facilities or lockers. Freezing will stabilize (stop) further water damage. Records can be kept in a frozen state for years. If the volume of damaged records is more than a few boxes or if the method of recovery requires shipment to a distant location, freezing may be necessary. Freezer trucks may be needed to move them to the cold storage facility or a recovery facility.

- Moving undamaged records off-site. If temperature or humidity can't be controlled, undamaged records will absorb moisture and, if conditions are right, mold will begin to grow within 48-72 hours (see box on mold). Undamaged records can be moved to a location unaffected by high humidity. (See Appendix C-3-5.)

D: SELECT DRYING AND REPAIR OPTIONS:

The next decision is to select alternatives for drying and repair of records. The majority of damage is from water. Although there may be other damage such as smoke, soot, dirt and contamination, these will often be combined with water damage. Repair and cleaning of documents usually occurs after the drying process. In most cases the selection of the drying alternative is the primary decision.

Factors to consider in selecting a method of drying:

- Volume of media – Is the volume such that the records must be stabilized by freezing before being dried; must they be shipped via refrigerator carrier to a large drying facility out of state; or can desiccation humidification systems be used on site?
- Type of media – Are coated papers, photographs, and linen drawings and books damaged that are best dried by certain methods?
- State and degree of damage – Is there fire, mud or contamination damage that requires cleaning the records before they are dried? How wet are the records, completely saturated or just wet on one or more edges? Are records moldy?
- Sensitivity of the media – Does the media have coatings or emulsions that may be salvaged only through certain drying processes?
- Location of the drying facility – Can the drying be done on site or does the material have to be shipped out of state in order to use the selected method?
- Reference accessibility – Is access needed during the drying process?
- Funds available - Cost may dictate what is possible.

For further information:

- Media Types - See Appendix E-1.

- Drying alternatives including definitions, descriptions, advantages and disadvantages - See Appendix E-2 regarding:

  - Air Drying
  - Interleaf Drying
  - Desiccant Drying
  - Freeze Drying (cold storage)
  - Freeze Drying (freeze dry chamber)
  - Vacuum Thermal Drying
  - Vacuum Freeze Drying

- Smoke damage, fire damage, and contamination: (See Appendix C-6.)

Decision Logic Charts:

Figure 6-a and Figure 6-b, below are diagrams illustrating the decision process for responding to both small and large scale disasters, especially in dealing with water damage. They show graphically how to select among the various drying/recovery options based on factors such as funds available, nature of the damage, recovery speed and the need for reference to the records during the drying process.

The diagrams are generalized. Decisions and actions may vary, depending on the specific nature of the disaster. The alternatives shown may be used in various combinations.

Small Disasters - One or two cabinets or a dozen boxes or less.
Usually can be handled by agency staff.

Large Disasters - Dozens or hundreds of cabinets or boxes.
Usually requires outside help such as temporary workers or disaster recovery firms.

A stabile environment means it is safe to enter and work in it. It also means environmental conditions such as humidity are normal.

If any of these conditions are absent, or if major repair or office rebuilding is necessary, all records may have to be removed.

Triage means dividing things into threes. Divide (1) Essential Records and other Important Records from (2) Less important records and (3) Records that are unnecessary or cannot be recovered.

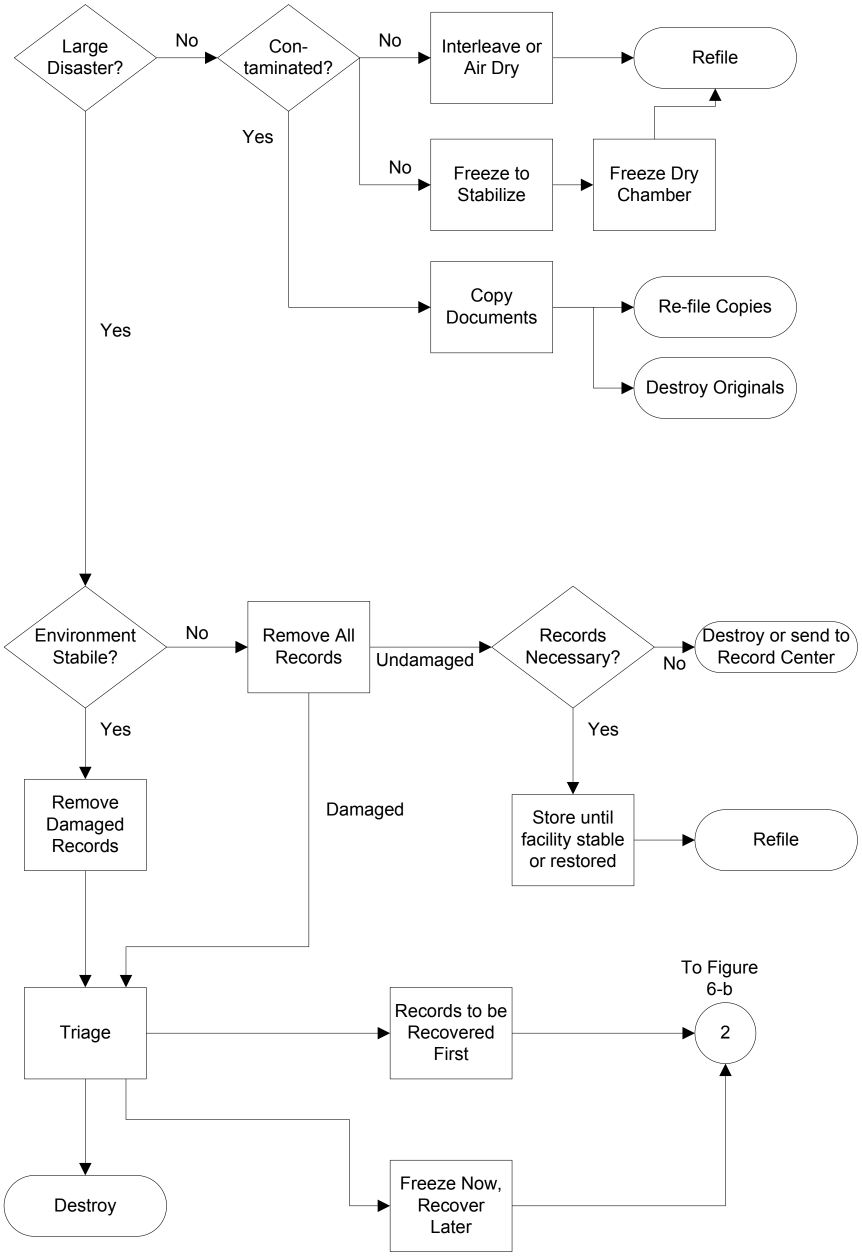
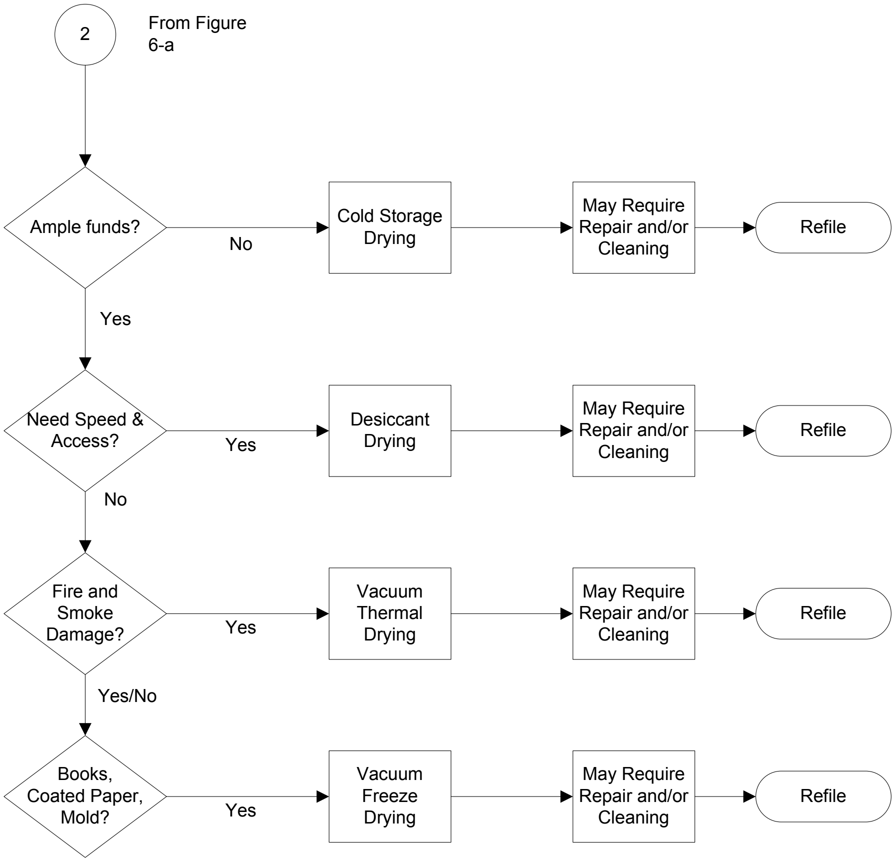


Figure 6a: Decision chart showing logic of selecting recovery/drying alternatives.

There will often be a need for improvisation. For example, in a recent disaster an organization was faced with the need to pay bills immediately. The normal procedure was to pay bills from original invoices but all the invoices were soaked. The solution was to copy the invoices while wet and pay from the copies. Clear plastic was placed over the copy machines to protect them from water during the copying process. The original invoices were eventually recovered by freeze drying.



Most local agencies do not have ample funds for document restoration. Cold storage drying is the least expensive solution for large volumes. It is very slow, and documents are not readily available for access.

Much faster than cold storage. Scalable to large volumes. Documents can be available for access. Expensive. Requires outside contractors. Does not always stop mold.

Good for fire damaged documents. Documents must be shipped to commercial facility. Expensive. Not readily available for access

Best solution for books and coated paper. Documents must be shipped to commercial facility. Expensive. Not readily available for access

Figure 6-b: Selection of Drying Alternatives

E. ASSEMEMBLE RECOVERY RESOURCES:

Based on the information gathered during the “walk through” including the volume of records damaged and extent of damage, stabilization and recovery method decisions, decide on and assemble the supplies, additional personnel, and contractors needed for the task.

- Employ the lists of staff, volunteers, or temporary help assembled in the plan. (See Appendix B-4.)
- Use pre-arranged spending and hiring authorities or work appropriate agency staff to provide personnel and emergency funds.
- Move pre-packaged supplies to the damage site, or use lists assembled in the plan to locate and acquire supplies and equipment needed. (See Appendix D-2, 3.)
- Implement pre-arranged contracts made with commercial recovery firms or contact such firms from lists assembled in the plan. (See Appendix D-4.)

CHAPTER 2 RECOVERING FROM RECORDS DISASTERS

A: RECOVERY DEFINED:

Recovery consists of actions and treatments that restore records and information to a useable state. Once recovery decisions have been made, recovery actions can begin. These activities may include, but are not limited to, one or more of the following:

- Implement a system for intellectual and physical control over damaged records.
- Pack out records.
- Stabilize by freezing for later recovery.
- Dry water damaged records.
- Clean documents soiled by dirt, mud, ash, soot, and mold growth.
- Store undamaged records.
- Repair documents charred by fire.
- Deodorize smoke-damaged records and fumigation for mold.
- Reprocess, clean microfilm and magnetic media.
- Duplicate contaminated or other badly damaged documents.
- Destroy unnecessary records or records too badly damaged to salvage.
- Repair and restore using conservation techniques for photography, microfilm, coated papers, maps, blueprints and drawings on sepia, linen or other textiles.
- Re-house returned records (re-foldering, filing, boxing, labeling, shelving, etc.).

Ancillary but related actions:

- Retrieve and install electronic record back-ups. (See Part I.)
- Use the Essential Records Schedule to determine if copies are available and where.
- Replace records with security copies.
- Use transmittal documents to determine exactly what is secured, where and who to contact for retrieval or copying.

B. RECOVERY RULES OF ENGAGEMENT:

1. DO NOT ENTER A DAMAGE SITE AND BEGIN REMOVING RECORDS WITHOUT A PLAN: Removing records without intellectual and physical control will result in chaos. No one will know who has what, where it has gone, and what has happened to it.

2. WORK SAFELY: Follow safety rules and instructions. There still may be remaining safety hazards such water soaked carpets, slippery floors, loose electrical wiring, and possible contaminants.

Wet records gain weight and expand in size, 200 percent of their original weight, and 30 percent in size. File drawers containing wet records may be difficult to open due to swelling. Forcing them open may cause additional damage. Lift smaller qualities of wet records than would normally be the case. Follow safe practices lifting boxes. Use a back brace.

3. BE AWARE OF CONTAMINATION: Contamination due to terrorism is a small, but increasing threat. Accidental contamination due to sewage pipe leaks, PCBs and mold are also dangers. If contaminates are suspected, see that the damage site is tested by appropriate state or local authorities such as the state Departments of Labor and Industries, Health, and Ecology. Follow

advice on handling specific kinds of contamination. Use rubber gloves and footwear, protective clothing and masks if necessary. See Part II, Ch. 2-D, and Appendix D for personal equipment and supplies.
Mold is the most common form of contamination and the most immediate danger to wet records. (See Appendix C–2, 2 for information about mold.)

4. KNOW WHAT YOU HAVE: Intellectual control over all records leaving the damage site is essential in order to know what records went where for stabilization, temporary storage, recovery or disposal, and to insure that recovered records are returned to their proper office, file system and owner.

A simple information system can be prepared as part of the detailed damage assessment or as records are boxed or crated for removal from the damage site. Tracking should be done at the box or crate level when removing records. If tracked at a higher level, pallet loads, for example, the boxes will be removed for whatever recovery action takes place, and not necessarily returned on the same pallet or even in the same load. Without a system, it will not be possible to identify the returned records and determine what additional cleaning or repair the records may require, or to where they are to be returned.

The system should identify 1) the office of record, record series, inclusive dates, 2) office location by file cabinet or shelf unit and drawer or box, 3) if the damage is due to water, fire or contaminant exposure. (See Appendix A-6, for inventory and tracking system form samples.) If the damage is limited to less that 10 or 12 file cabinets or 100 boxes, a manual system may be adequate. An automated system has great advantages for larger disasters. It can be a simple system based on a PC spreadsheet or database. An automated system will also be useful later for audit and insurance reports, destruction reports etc.

C. BASIC RECOVERY PROCEDURES

PACKING OUT: "Packing out" is the term used for boxing, crating, labeling, and moving records out of a damage site.

1. What to pack out: This depends on the conditions of the disaster and methods of recovery selected and the re-prioritization described in Chapter 1.

As a general rule, pack out and recover essential and valuable records first. However, the disaster recovery team must also be concerned with all records in the damage site. Valueless records suddenly become important as a nuisance and cost factor if they must be moved out of the way for reconstruction or repair of the facility or for shredding, or must be removed because of mold growth.

Undamaged records may be destined for storage, but if they have been in an environment conducive to mold growth, their presence at a records storage facility may be refused.

2. How to pack out: Different recovery methods may mean different packing out practices, containers and supplies. Commercial records recovery services will probably recommend and sell appropriate containers. Use information in Appendix C-4 if you are "on your own" or using a public or private service that does not have specific container requirements.

See Appendix C for detailed specific instructions for packing out, rinsing, cleaning, inter-leaf, and air drying and repair of damaged documents and books.

See Appendix C-6 for recovery from fire damage.

See Appendix E-2 for drying alternatives including definitions, advantages and disadvantages of each.

ADDITIONAL INFORMATION IN THE APPENDIXES: Specific procedures for the basic recovery of different media and formats of records are covered in Appendix C. The records disaster recovery team should be trained in their use and have them available when going into a disaster site. Appendix C contains a series of procedures and instructions that may involve commercial services but stress recovery employing the disaster recovery team and agency staff. These appendices and templates can be adopted as is, or may be tailored to the agency and cover the following:

- Recovery of paper records damaged by water, fire, mold, or a combination thereof: Appendix C-5 and C-6
- Recovery from Contamination: Appendix C-7
- Recovery of films and photograph materials damaged by water and fire: Appendix C-9
- Recovery of electronic records damaged by water, fire or contamination: Appendix C-10

Procedures for records recovery should be in the Team Members' Records Emergency Response Packets. Training should be offered to Team Members and other agency staff in these actions, techniques and treatments.

D. POST RECOVERY -- DISASTER FOLLOW-UPS & DOWNS

Records trauma: Disasters traumatize records. They will rarely be the same again. Water, and even over humidification, will cause paper to curl, wrinkle and swell, certain inks to run, and result in mold damage. Fire and contamination can have other effects. Don't expect records to be returned from recovery looking like they were before the disaster. Most of them will be stable and useful, but not "as good as new" (see repair and conservation).

Additional file cabinets will be needed for the same records.

Dried records will have a larger volume than before the damage. More file space will be needed than before. Drying causes paper to contract, but leaves air spaces between what were previously close spaced fibers.

1. Re-shelving recovered materials

- Records storage areas should be repaired using fire resistant materials.
- Cleaning personnel should sterilize the area to destroy any mold (in cases of water damage).
- Closely inspect the site to insure that there will be no residual moisture or signs of mold.
- A healthy environment for records includes a stable temperature (50˚to 60˚ F) and relative humidity (35 percent to 45 percent). Offices and file rooms are not normally kept at those levels. Higher temperatures and humidity will promote mold growth, particularly in previously damaged or moldy records.
- Regular inspections should be scheduled for at least one year following the return of damaged materials to the storage area. A random sampling technique may be used in inspecting the affected materials.

2. Recovery analysis and reporting

- Determine the cause of the disaster so that precautions can be implemented to prevent a recurrence.
- Hold a meeting of the records disaster recovery team members. Discuss all aspects of the experience.
- Report lessons learned. What went right and what went wrong?
- Evaluate existing preparedness, response and recovery plans. Identify what parts need updating or changing;
- Note which, if any, contractors, suppliers, or facilities proved inadequate;
- Determine what will be included in a report detailing the cause of the disaster and the response and recovery procedures used. (This report will serve as a reference and planning tool preparing for future records and information disasters.)
- Prepare a general summary of the response and recovery operations.
- Prepare a detailed report.

3. A letter of thanks should be sent to all individuals and agencies that participated in the response and recovery operations.

SUMMARY

- Prevention is more effective than recovery. Anyone who has experienced a records disaster understands recovery is messy, expensive, labor intensive, time consuming and sometimes an impossible task.

- The Essential Records Program is the heart of prevention and protection.

- Duplication (backup) is the best form of protection.

- Protection is especially important for electronic records. Recovery of damaged hardware, software and data is problematic. Backup is the first line of defense. It is increasingly practical for even small agencies to employ advanced backup techniques.

- When a disaster strikes, the response must be fast and sure. Speed is critical.

- In order to respond with speed, accuracy, and coordination, there must be a Records Disaster Plan in existence prior to the disaster. The plan should cover policy, authority, responsibility, communication and funding, as well as techniques.

- The plan can be part of the overall agency disaster plan, or it can stand alone. It should harmonize with, but not duplicate, agency disaster plans or electronic systems disaster plans.

- The response effort must be led by a person or a team who understands records.

- In order to set priorities and make response and recovery decisions correctly, the agency must know what records it has and understand the recovery alternatives and how to use them.

- The recovery plan of action used in a disaster, although based on the Records Disaster Plan, will be fine-tuned based on actual circumstances. There probably will be improvisations. Plan strategically, be flexible.

- Disaster response and recovery plans should be tested periodically.