Transforming Lives

Building an Essential Records Protection Plan

Protecting DSHS records
needed for continuity of operations
during and following a disaster.

Washington State Department of Social & Health Services
Transforming lives

Mission Essential Functions

DSHS Emergency Management Services has identified DSHS mission* essential functions for each administration which include:

- Emergency hiring
- Payroll processing
- Mail processing
- 24/7 residential care for clients
- High Risk community services case management
- Foster care support
- Food and cash assistance

All of these essential agency functions require records. Those records which allow DSHS programs to conduct business under emergency conditions and resume more normal business afterward are called **essential records**.

* For further information regarding the DSHS mission, vision and values, go to https://www.dshs.wa.gov/strategic-planning/mission-vision-and-values.

Essential Records

Without essential records, daily agency business would stop. DSHS could be vulnerable to:

- Litigation;
- Unplanned expenses of financial settlements or revenue loss;
- Disruption of efficiency due to gaps in information; and
- Breaks in the continuity* of operations.

Essential records allow DSHS to continue functioning under adverse conditions regardless of intensity and duration.

Agency staff must ensure these records are not only protected from the effects of an emergency but are also accessible during and after an emergency.

For further information about essential records, go to About Essential Records, a PowerPoint presentation designed to describe and introduce conversations to have about essential records.

* Business continuity is a plan to help ensure that business processes continue during an emergency or disaster.

Call to Action

The first action to developing strategies for the protection of essential records is inviting the appropriate staff to the table. Discussions should include the following staff:

- Office and line;
- Information technology;
- Records management; and
- Emergency management.

These should be staff who:

- Are familiar with program records and processes.
- Know where and how program records are kept and retained.
- Understand legal retention requirements.
- Manage agency / program response during an emergency.
- Have authority to implement an essential records plan.

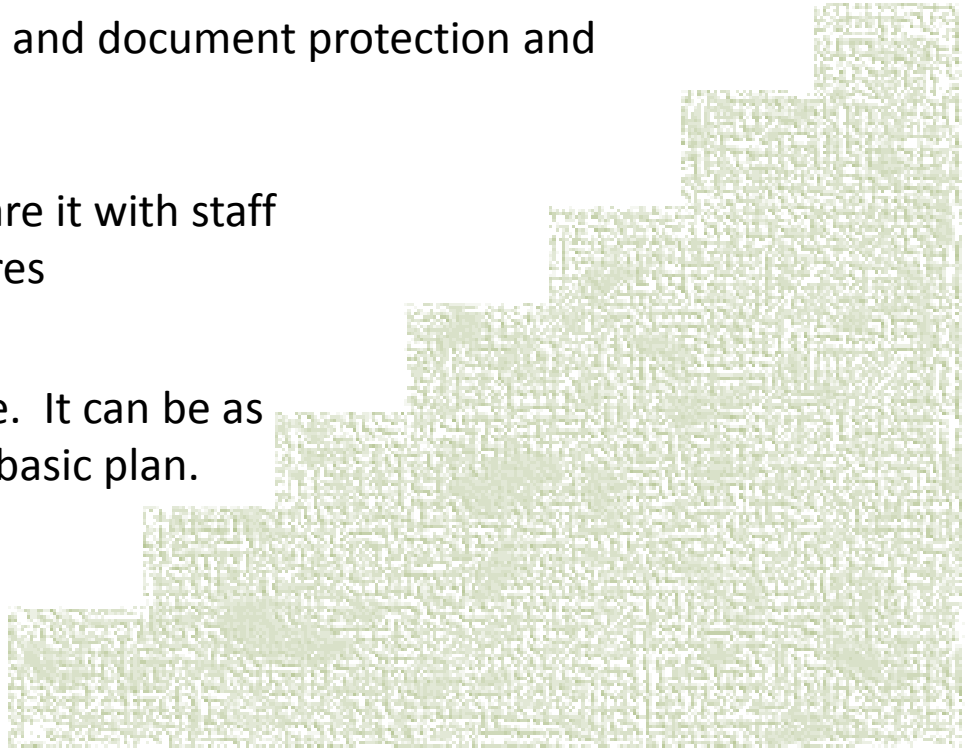
Elements of a Plan

The following steps are offered as guidelines to help your work group develop a protection plan for your office.

1. Identify and list your essential records
2. Know where to find your essential records
3. Assess potential emergencies, and document protection and rescue strategies
4. Discuss what can go wrong
5. Write your plan down and share it with staff
6. Implement protection measures
7. Review annually

Your plan doesn't have to be huge. It can be as simple as listing and publishing a basic plan.

The best way to start is by taking the first step.

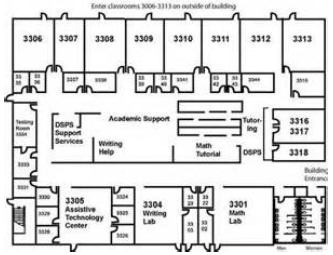


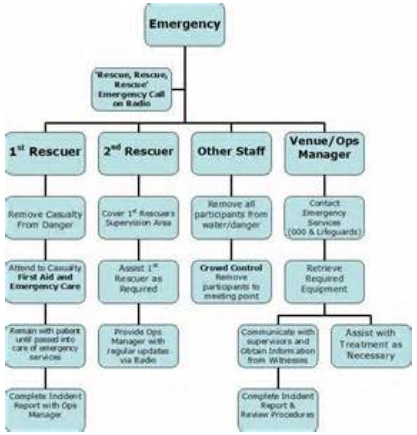
1. Identify and list your essential records

Identify **and list** your office essential records. For disaster recovery records, there are two types to consider, **emergency response** and **continuity response** records.

Emergency response records are necessary at the time of or shortly after an incident and include emergency action plans, essential records inventories, emergency management staff and contact numbers. Examples of **emergency response records** include:

- Maps
- Building plans
- Emergency plans
- Contact information
- Delegation of authority





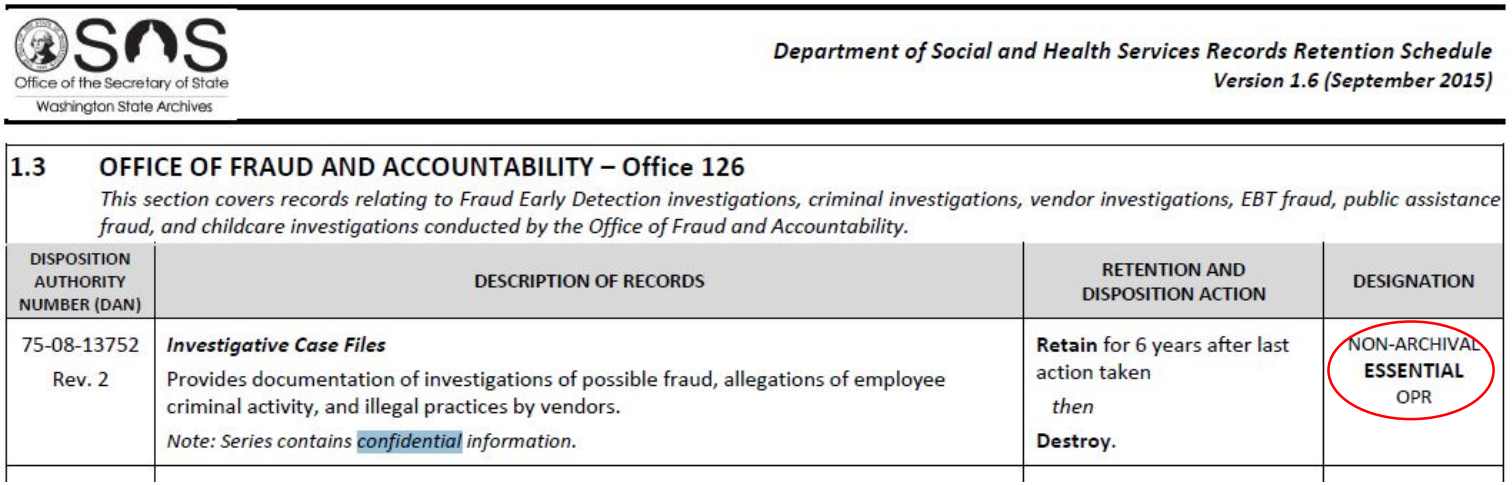
Continuity response records are required for agency legal, financial and public responsibilities. These records are required in order to keep your program functioning for as long as the emergency lasts and help you resume normal business activities, and include:

- Client case records
- Patient and resident files
- Accounts receivable
- Payroll records
- Provider files
- Contracts and agreements

You should also include:

- Physical lists and locations of these records
- Staff responsible for these essential duties
- Software source codes
- Access and permissions lists

Both the State General Records Retention Schedules and the unique DSHS Retention Schedules identify essential records under the Designation column. For example:



Office of the Secretary of State
Washington State Archives

Department of Social and Health Services Records Retention Schedule
Version 1.6 (September 2015)

1.3 OFFICE OF FRAUD AND ACCOUNTABILITY – Office 126

This section covers records relating to Fraud Early Detection investigations, criminal investigations, vendor investigations, EBT fraud, public assistance fraud, and childcare investigations conducted by the Office of Fraud and Accountability.

DISPOSITION AUTHORITY NUMBER (DAN)	DESCRIPTION OF RECORDS	RETENTION AND DISPOSITION ACTION	DESIGNATION
75-08-13752 Rev. 2	***Investigative Case Files*** Provides documentation of investigations of possible fraud, allegations of employee criminal activity, and illegal practices by vendors. *Note: Series contains confidential information.*	**Retain** for 6 years after last action taken *then* **Destroy.**	NON-ARCHIVAL **ESSENTIAL** OPR

Additionally, essential records may contain confidential or sensitive information which require special handling. If a record is confidential, this will also be listed in the records retention schedule.

NOTE: The State General Records Retention Schedules contain retention for records common to many state agencies and include administrative, fiscal, legal and personnel records; while the unique Department of Social and Health Services Retention Schedule contain agency-specific records retention schedules that are unique to DSHS.

Questions to ask:

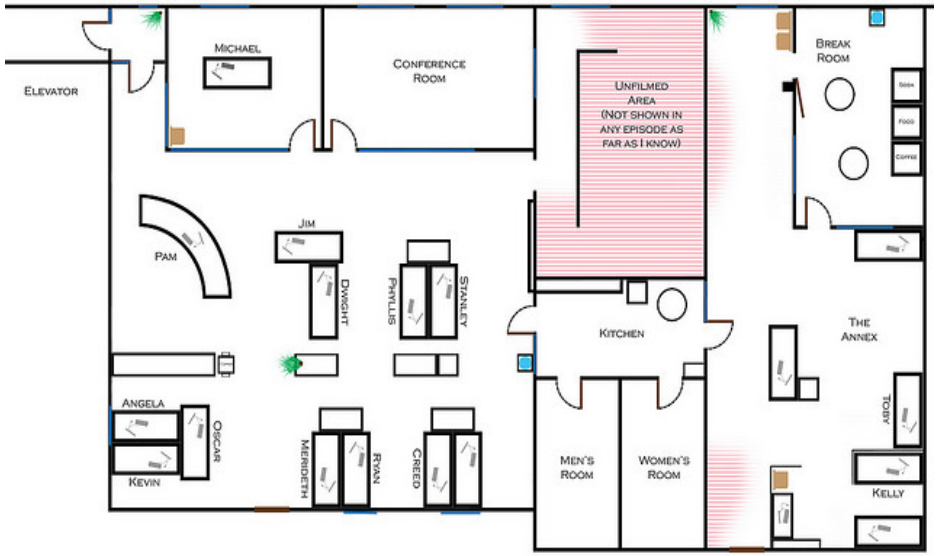
- ✓ What records do we need to continue our work? For one day? For one week? For one month?
- ✓ Which of our records protect the rights, privacy or interest of DSHS, its staff, or our customers? Or show that the agency is owed or owes money, goods, or services?
- ✓ Do these records assist recovery in the event of a disaster?
  - Which are needed for emergency response procedures?
  - Which are needed for continuity of services?
- ✓ Which of our essential records are also archival?
- ✓ Where is our essential records list located?
- ✓ Who is our Records Coordinator?
- ✓ Who has authority to send non-essential staff home and what do we do if that person can't be reached?

2. Know where to find your essential records

Once you identify your essential records, you need to know where to find them. Add this information to your list of essential records.

Know if these records are:

- Originals or copies.
- Available as electronic records on servers or backup tapes.
- Located on shelves, in vaults, or file cabinets / drawers as paper records.
- Available anywhere else in the agency.
- Accessible in an emergency.
- Located at the [State Records Center](#).



Draw a map showing where in your office your essential records are located and include a copy in your records disaster plan.

If your essential records are located in your office, keep them together and separate from other records. This ensures they can be found during an emergency, and be easier to find and move as needed.

- If possible, locate them near a exit to ensure easy and quick access should you need to physically move your office.
- Protect on-site records in vaults or fire-resistant containers.
- Aisles and doorways should be kept clear at all times.
- Staff members should know the location of all ABC fire extinguishers and understand how to use them. ABC fire extinguishers deal with three types of flammable materials: A - wood and paper, B - liquids and grease, C - electrical.
- Basements or ground floor areas should be used for storage as a last resort since they are most susceptible to water and sewer damage.






Create electronic versions for easier back-up and access during an emergency.

If possible, arrange off-site storage for back-up tapes or imaged hard-copy documents.

- Your plan must include how to retrieve these records when needed.

And, don't forget archival records!

Archival records may not be needed immediately, but we are legally responsible to ensure protection and rescue. Examples of records which are both essential and archival include:

- Rule making files
- Institution admission and discharge registers
- Master patient indices

It is strongly recommended that you use the SRC to store paper records.

The State Records Center provides low cost, secure storage in a safe environment; and returns records quickly when you need them – even in an emergency.

For convenience, include records retrieval procedures in your records protection plan. Additional information about Using the State Records Center, may be found at http://one.dshs.wa.lcl/FS/Loss/Records/Pages/Training.aspx.

Questions to ask:

- ✓ Can we easily find and access our essential records?
- ✓ Do we have off-site and out-of-region contacts for storage?
- ✓ Is the equipment or area used for storage adequately safe from disasters and unauthorized access?
- ✓ If our backup records are off-site, are they easily accessible for key staff?
- ✓ Are our backup facilities located:
  - In separate geographical areas from our primary work area?
  - On a different power grid than our usual facility?
- ✓ Which of our essential records are also archival?
- ✓ Are we sending archival records to State Archives?
- ✓ Are we using the State Records Center to store inactive records?

3. Assess potential emergencies, and document protection and rescue strategies

Brainstorm disaster scenarios: discuss protection methods by determining what emergencies you may face. **No one solution will work for all emergencies.** Decide which emergencies are common to all and which are specific to your geographical area.

Localized emergencies for all of us include fire and water damage, electrical failure, equipment or software failure, and human error.

Depending on your physical location, wide-spread Washington State emergencies include earthquakes, floods, wind and ice storms, and volcanic eruptions!

Additionally, government agencies may also experience civil emergencies or malicious computer attacks.

The Federal Emergency Management Agency (FEMA) recommends to reducing vulnerability after determining which records, files, and materials are most important to continuity of services by considering different types of disasters (such as floods, hurricanes, and earthquakes), and take steps to protect these records, including the following:

- Raising computers above the flood level and moving them away from large windows
- Securing equipment that could move or fall during an earthquake
- Consider off-site protection plans such as planned dispersal, E-vaulting, or duplication of records
- Regularly backing up essential electronic files and storing backup copies in a secure off-site location
- Moving heavy and fragile objects to low shelves
- Purchase fire-resistant cabinets and vaults.

Water, fire, and smoke damage should receive particular attention as they present the greatest danger of damage to records. **Nearly every records disaster comes down to one thing: water.**

Water risks include leaking or breaking water pipes, heavy rains and floods, or sprinklers triggered by a fire.

Moisture in any form and paper don't mix; when exposed to water, paper begins to deteriorate. Mold and bacteria appears within 48 hours in warm weather.

Immediate action is required in order to mitigate water damage:

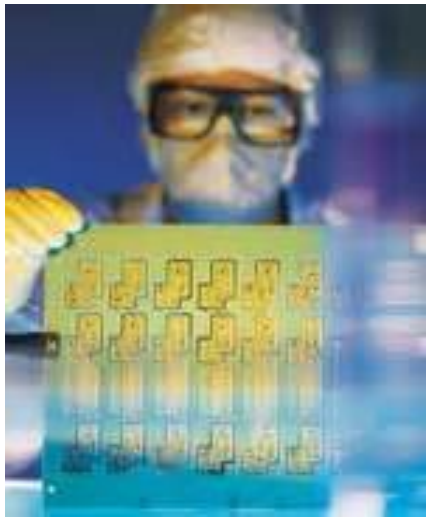
- Keep water-soaked records as cool as possible with good air circulation.
- Use dehumidifiers in small, enclosed areas or fans to circulate air.
- Remove standing water.
- **Get immediate help from professionals.**

Simple preventive measures such as closing filing cabinets, keeping your records off the floor, and putting your records away at night help mitigate the risks of after hours water emergencies.

The Department of Enterprise Services has contracts in place for document recovery services for use by state and local government agencies. Details may be found at their website:

https://fortress.wa.gov/ga/apps/ContractSearch/ContractSummary.aspx?c=01112

In the event your office must contact document recovery vendors, call one of the following vendors **as soon as possible to mitigate damage**. Your organization is responsible for costs incurred.



- BMS CAT, Inc. at 253.709.8677 or 800.422.6379
- Polygon US Corporation at 562.6322

Both vendors:

- Perform drying and restoration services in-house and on-site.
- Give immediate, short-term preservation instructions for small or large water emergencies.
- Arrange recovery of damaged records.
- Adhere to confidentiality and security requirements.

Questions to ask:

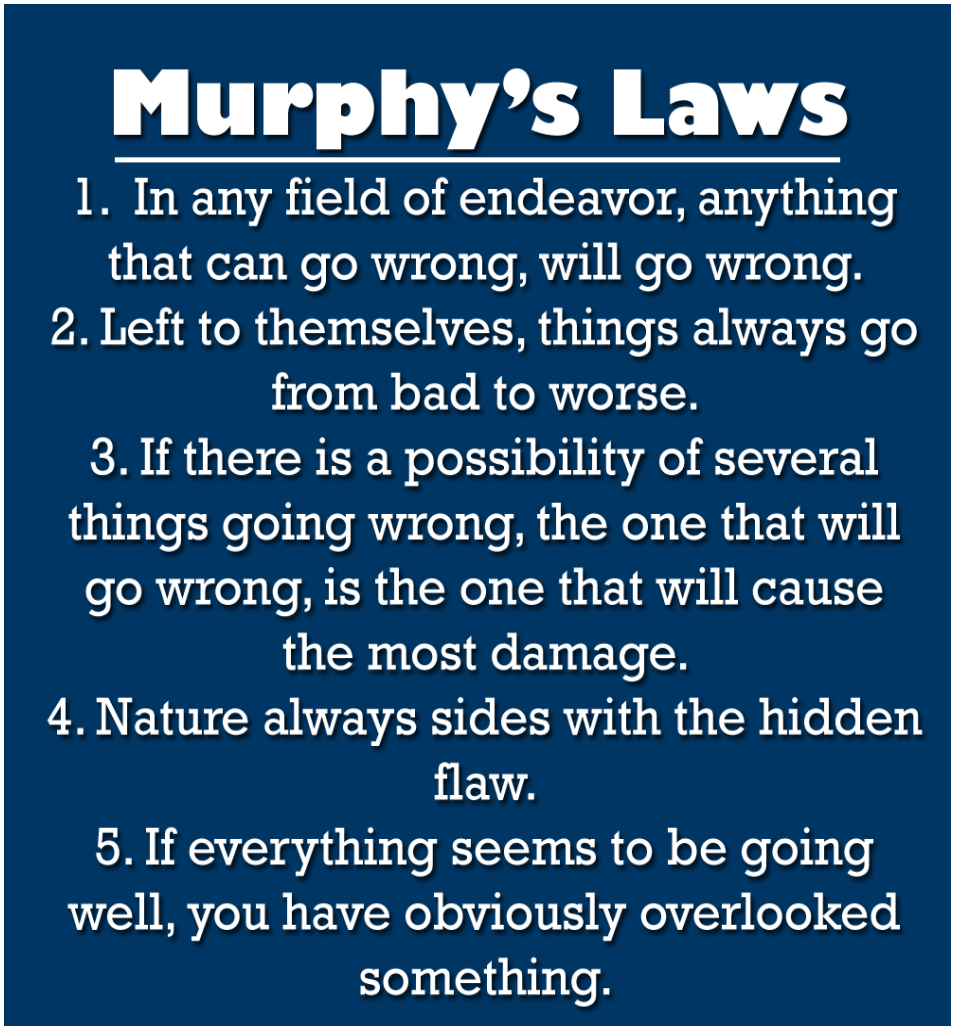
- ✓ How do we want our staff to respond to a:
  - Fire emergency?
  - Water pipe leak?
  - Earthquake, etc.?
  - Bomb threat?
  - Computer virus?
- ✓ How is our building secured against fire, flood and other disasters?
- ✓ What security measures do we have to stop unauthorized entry into a records storage area?
- ✓ During an emergency, who should be doing what?
- ✓ Do our staff know what to do in a situation involving an active shooter?

4. Discuss what can go wrong

Contingency planning is an important consideration of essential records protection.

Expect the unexpected.

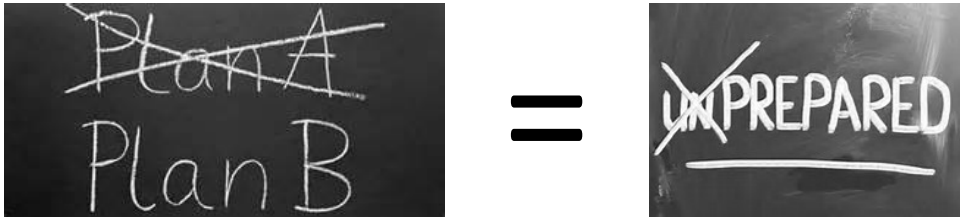
Developing an effective "Plan B" is essential as many things can go wrong in an emergency situation. Discussing and writing contingency plans prepare your office for such possibilities while helping to identify current risks.



Brainstorm disaster scenarios and devise plans for each scenario. **Find ways to reduce immediate risk.**

- Assess how you can take steps now to reduce your risks in each of your disaster scenarios (i.e., office clean-up helps alleviate risks for fire and water damage).
- Develop preventative strategies and plan for back-up staff to ensure someone will be available if originally identified staff can't be located.
- Consider the availability of partners.
- Find out-of-area locations for data storage if on-site records cannot be accessed.

Contingency plans help identify areas needing improvement. You might realize you should have disaster drills or that key staff need additional training.



Questions to Ask:

- ✓ What if emergency response team members cannot be located?
- ✓ Do we update our essential records to ensure they contain the most current information?
- ✓ What can be done if resources cannot be located to help with water damage?
- ✓ What happens if we can't get into the building for our essential records?
- ✓ What is the protocol when there is no electricity or auxiliary power? Will we be able to get into the building?
- ✓ What local resources would be available if the disaster struck?
- ✓ What can we do now to help prepare for emergency operations?
- ✓ Where are our back-up records located?

5. Write your plan down and share it with staff

The most important implementation to establishing a plan to help protect and access your essential records is to **WRITE** it and **SHARE** it with staff.

Communicate your emergency plan to all employees.

- You need to educate key people before it's ever needed.
- Tell people which role and responsibilities they will have so there's no confusion if the plan needs to be implemented in an emergency. An understanding of what is expected reduces panic and helps create a safe environment for staff.
- Share existing resources, for example, the Emergency Information Hotline for Employees: **1-866-DSHS-EMP** and the list of office closures.
- Give people the proper training they will need to meet their obligations as outlined in the plan. Hold drills if needed.
- Make adjustments after observing training.

Questions to Ask:

- ✓ Do staff and managers know where our essential records list and protection plan are located?
- ✓ Are new employees, including new managers, educated on our essential record protection measures?
- ✓ Do staff and managers know who is responsible for implementing our emergency procedures?
- ✓ Do staff and managers know of our off-site storage for essential records?
- ✓ When was our last essential records discussion?

6. Implement protection measures

You can make changes now which doesn't require money or expensive equipment; but help to protect the agency's essential records.

Transfer essential records to the State Records Center as soon as possible. Reduce the time these records are kept in the office to the minimum, consistent with retrieval needs.

The following are examples of simple ways to protect essential records kept on-site:

- **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 and continuity team members.
- **Keep essential records separate from other records**. They will be easier to find during an emergency.
- **Keep essential records close together**. They will be easier to find and move.

- **Locate essential records as close to the door as possible.** Easier to remove quickly.
- **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.
- **Keep essential records off the floor.**
- **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.
- **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.

- **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.
- **For electronic records, or imaged hard-copy documents, store back-up disks at an off-site location.**
- **Consider microfilming your essential records.** Microfilm is an affordable medium for duplicating essential records. Microfilm requires no hardware and software to read and is legible to the naked eye with only the aid of a magnifying glass. It stores compactly and is cost-effective.
  - Over 4000 documents can be stored on a 16 mm reel of film the size of a small box of crayons.
  - Each page can be duplicated for only a few cents.

  Washington State law provides for these copies to be accepted as originals in court. **State Records Management will store microfilmed records free-of-charge.**

Questions to Ask:

To maximize the success of your essential records protection plan, consider:

- Is your backup data:
  - ✓ Located off-site?
  - ✓ Updated frequently?
  - ✓ Secure?
  - ✓ Accessible?
- Is your staff:
  - ✓ Involved in the planning?
  - ✓ Consulting about what is important?
  - ✓ Trained about expectations and who is in charge?
- Is your plan:
  - ✓ Reviewed and tested as often as practical?
  - ✓ Documented?

7. Review annually

Review your emergency plan annually or when responsible staff change and update as necessary.

A key piece of designing a essential records protection plan is to review it to ensure your processes are still applicable to your staff and location, software and hardware, and your business processes.

At least annually, review your:

- Essential record lists
- Maps locating essential records
- Record rescue and accessibility strategies
- Equipment storing records, electronically or hard copy
- Disaster recovery contact information
- Staff emergency training plan
- Office environment
- Off-site storage and back-up
- New offices or staff

Have a plan.
Write it down.
Share it with staff.

Take the first step; and, remember, your plan doesn't have to be comprehensive. Begin with the basics and add to the plan over time. Make it a living document which can be changed and improved with experience and annual review.

Following are examples of two plans contributed by the Language Testing and Certification Program and the Division of Vocational Rehabilitation, headquarters office.

Take the first step.

Language Testing and Certification Program (FSA/OSSD/OAR)

1. **Which of the records we use are essential?**
   - Master voice recorded tests
   - Master written tests
2. **Where can we find our essential records?**
   - We can find the master voice recorded oral tests in the fire-safe cabinet located in the LTC records room.
   - We can find the master hard-copy written tests in the fire-safe cabinet located in the LTC records room.
3. **What are our actual risks?**
   - Earthquakes
   - Technological emergencies
4. **How can we protect our essential records?**
   - Keeping them safe in one constant spot.
5. **What is our Plan B?**
   - We have master files stored on ISSD servers of the oral tests and written tests.
6. **How should employees respond to an emergency?**
   - Since our records are in a fire-safe box, we should not worry about finding and taking records with us during an emergency.
7. **Where are our essential records located? What security measure do we have to stop unauthorized entry into a records storage area?**
   - Our tests are under lock and key in the safe, located in the LTC record room, which is kept locked at all times.

DVR State Office Protection of Essential Records and Backup Plan (Disaster Recovery Plan)

When a disaster breaks out, the protocol below are measures to ensure that our records and essential records are protected, in case of a disaster, such as a fire, earthquake, flood, etc.:

1. The DVR S/O records are kept in locked metal cabinet files, where they are secured.
2. The keys to the cabinets are kept in a secured place where they are accessible in case of an emergency.
3. The cabinet files are located near each unit areas to locate easily when needed in case of an emergency.
4. Each person responsible for the keys to the cabinets, has a designated backup person to locate the keys, and the primary's person phone number for emergency contact.

Have a plan.
Write it down.
Share it with staff.

6. DVR S/O sends essential records to SRC every 4 to 5 months to clear them out of the office to protect them from fire, flood or earthquake. Our cabinet drawers would be damaged if experienced a flood or fire disaster.
7. DVR S/O building is constructed to handle an earthquake. The building will just sway from one side to another.
8. Our primary IT person is the contact for the electronic essential records that maintains the backup files in our shared drive under secured folders for DVRs essential records. Our shared drive is constantly being backed up. Management is our IT backup to ensure protection of electronic records in case of emergency.

Resources: Information

For information about protecting Essential Records:

- RCW 40.10.010 Essential records – Designation – List – Security and protection - Reproduction
- Essential Records and Disaster Preparedness Manual http://www.sos.wa.gov/archives/RecordsManagement/EssentialRecordsDisasterPreparednessManual.aspx
- Disaster Preparedness, Response & Recovery - Advice and Resources, Office of the Secretary of State http://www.sos.wa.gov/archives/RecordsManagement/DisasterPreparednessandRecovery.aspx
- Millie Brombacher, Agency Records Officer or your local Records Coordinator.

Transforming Lives

Be prepared.

Robert Baden-Powell, Founder
Boy Scouts of America