APPENDIX B
RISK ASSESSMENT TEMPLATES

Appendix B provides procedures, forms and suggested lists of records for developing an essential records protection program. It recommends methods of backing-up and restoring electronic records when there is no established information technology department or existing electronic records protection plan. Prevention procedures and risk assessment checklists are also contained in this appendix.

Use this section to document your plans for protecting essential records, and the identification, reduction and mitigation of disaster hazards. Use the physical plant risk assessment inspection checklists to conduct an assessment to identify your vulnerabilities and needs before preparing these plans.

B-1 Essential records Protection Policy and Procedure Model

PURPOSE: Essential records protection is a major part of an overall preparedness and recovery program for disasters that affect Agency records.

The Essential Records Protection Plan is a procedure for protecting the _____ (insert agency's name) vital records from disaster. It consists of a schedule which identifies records essential to the operations of the agency during an emergency, and those records essential to the recovery of normal operations after a disaster. The schedule specifies how those records are to be protected, and establishes how often they are to be updated or cycled.

POLICY: It is the policy of the (insert agency name _____ to:

Insure the protection of records deemed essential to the functions of the agency during and emergency, and to restoration of normal operations afterward.
   o   Records needed to protect the rights and interests of the public served by the agency;
   o   Records needed to protect the rights and interests of the agency as a government entity;
   o   Records necessary to fulfill the department's obligations to employees;
   o   Records needed to protect the legal and financial integrity of the department's programs;
   o   Records required to maintain the technical ability and efficiency of the Department;
   o   Records, the loss of which would make resumption of operations prohibitively expensive or impossible.

SCOPE: This policy affects all employees who have records keeping responsibilities.

REPONSIBILITY:
The agency records disaster recovery coordinator will:
• Assist departments in the identification of their essential records;
• Assist departments in determining methods of replication and protection that are cost effective;
• See that the essential records schedule is updated annually;
• Maintain the official copy of the essential records plan;
• See that records are replicated appropriately, sent to storage on time, and cycled out of as scheduled;
• See that essential records being sent for security storage are properly documented, boxed and labeled.

PROCEDURE:

Updating the Essential Records Schedule
- Each year, the disaster recovery coordinator or records manager will send a memo to all program directors requesting that their program's essential records schedule is updated.

- Departmental recovery coordinator reviews the schedule with the department director.
  This review should consist of an administrative evaluation of whether each record series listed on the schedule continues to merit inclusion and the attendant costs of replication and storage, if any. This evaluation should consider the agency's policy stating what types of information requires protection.

  The review should include consideration of any new records series developed as part of new or added program functions; and should consider new and less costly methods of replication resulting from the application of technology.

- Changes, additions and deletions to the essential records schedule can be made by annotation directly onto the current program schedule form. If additional space is needed, use a new schedule form. Make sure the following information is correct for each record series:

- Record titles identify the records series by title and Disposition Authority Number from the Records Retention Schedule.

- Media indicate how the records series will be replicated for security storage, such as hardcopy, computer output microfilm, floppy disk, CD, microfilm, etc. Consult with the records manager for advice and assistance on replication. A series may already be replicated and secured electronically or may be easily be secured if the information is on an electronic system.

- There are several methods of providing security copies of essential records. Usually no one method will suffice for all records. Consider the following questions in making a decision. Each record series should be examined in terms of:
  - frequency of use
  - useful life of the media
  - availability of existing copies
  - volume of the records involved
  - and the cost of copying and storage

    Use of existing copies protected through natural dispersal. Some records exist in multiple copies. One of these copies can be designated as the essential record protection copy for such records.

    Paper Duplicates - Where copies do not already exist, the production of additional hardcopies of a record identified as essential may be merited. This is practical when the *volume is minimal* or the *update cycle is frequent*
    Microfilm or computer output microfiche - These methods are most commonly used for providing security copy of records which are voluminous, not superceded or updated frequently and have long term or permanent value.
    Electronic Media - This method is best used when the essential record is already in electronic form; volume makes paper copy impractical, and when the information is frequently updated or superceded.
    Update Cycle - Indicate the frequency that the record series is to be supplemented or superceded. It is important to establish an update cycle as frequently as practical in order to keep the

information or data current. Consult with the agency IT department or records manager regarding update cycles for electronic records.

Security Storage Site - Indicate the security storage sit to which each essential record series is to be sent. Use the following abbreviations:

- ER for electronic records sent through department to a designated security site.
- RC for paper and microfilm copies of essential records to be sent to the DCLU records center or through the records manager to the Washington State security microfilm storage site.
- ND for natural dispersal. Indicate the office which has the security duplicate.

Methods of Security Storage
- Natural dispersal
- Remote or off-site storage
- On-site storage

Sign-off - The updated schedule must be signed by the Program Manager.

Transferring essential records to security storage sites

Electronic Records
Essential records in electronic form on systems managed by the Department will be transferred to security storage by automatically according to the cycle established on the Essential Records Schedule.

Microforms
Essential records in microfilm or microfiche form are to be boxed in acid free microfilm containers (special order).
Label the containers as follows:

RECORD SERIES TITLE
Inclusive dates of records in the container
Department or office of record
Retention time in security storage

Send the boxed film and to the agency records disaster recovery coordinator.

Paper Records
Essential records to be secured in paper form are to be boxed and labeled using the agency or commercial records center storage boxes and labels per instructions for transferring records to off-site storage.

Except for essential records in electronic form, all records transferred for security storage must be accompanied by a completed Records Center Transmittal form. Annotate the form to identify the materials being sent as being for "Essential Records Security Storage."

Cycling essential records
Some essential records will continue in security storage with periodic accretions. Others will be cycled out and replaced with updated material per the Essential Records Schedule. Records scheduled for cycling out will be returned to the office of origin, or destroyed as indicated on the schedule when superceding records are received by the records center. Electronic records will be erased by agency when scheduled for replacement.

CITY OF WEST BALLARD

ESSENTIAL RECORDS SCHEDULE

1. ITEM NO.	2. RECORD SERIES TITLE	3. MEDIA	4. UPDATE CYCLE	5. RETENTION	6. PROTECTION INSTRUCTIONS
1	City Council Minutes	Microfilm	Annually	Permanent	Send security copy of microfilm to State
2	Ordinances and Resolutions	Microfilm	Annually	Permanent	Archives security storage in Olympia.
3	Annexation Files	Microfilm	Annually	Permanent	Send security copy of microfilm to State
4	Franchises	Microfilm	Annually		Archives security storage in Olympia
PROGRAM	**PROGRAM DIRECTOR APPROVAL**		**DATE**		**Disaster Recovery Coordinator or Records Manager.**

B-3 Essential records from the State General Schedule for Local Agency Records that your agency may hold.

FUNCTION and RECORD SERIES TITLE   METHOD of PRESERVATION

Accounting
      Time Accumulation Reports (Time Cards)   Microfilm
      General Ledger   Backup tapes off-site storage
      Individual Employee Pay History   Microfilm
      Journal Vouchers & Indexes For Electric Utilities   Microfilm
      Payroll Register   Microfilm
Administrative Records

Official Agency Policy & Procedure Directives Rules & Reg.	Microfilm
Cemetery Records	
Index of Interments	Microfilm
Section Books	Microfilm
Section Maps (sold & available lots and occupied lots)	Microfilm
City & Town Clerks	
Adopted Agency Policy & Procedure Directives, Rules, Reg.	Microfilm
Agency Charters (rights, responsibilities & authority)	Microfilm
Annexation History Files	Microfilm
Encroachments	Microfilm
Franchises	Microfilm
Minutes Official City/Town Council, Board, Commission	Microfilm
Oaths of Office	Microfilm
Ordinances & Resolutions	Microfilm
Records of Public Hearings (transcripts, speaker, testimony)	Microfilm
Communications	
Computer Automated Dispatch Backup Tapes	Backup tapes off-site storage
Conservation Districts	
Agreements With Landowners--District is Signing Party	Paper copy off-site storage
Long Range Plans	Paper copy off site storage
County Coroner & Medical Examiner	
Card Index File	Microfilm
Coroner/Medical Examiner Ledger (chronological & alpha.)	Microfilm
Coroner/Medical Examiner Investigation Files	Microfilm
Inquests	Microfilm
Electric Utility Operations	
Maps & Area Plats	Microfilm
Pole List (pole type, location, ancillary equipment, etc.)	Microfilm
Staking Sheets (power line construction or extension)	Microfilm
Standards & Specifications Manual	Paper copy off-site storage
Transformer History Data	Microfilm
Underground Line Files	Microfilm
Water/River Flow Reports	Microfilm
Electronic Information - System Documentation	
Electronic Information System & Software Backup Data	Microfilm
Electronic Information System Design Documentation	Paper copy off-site storage
Electronic Info. System Programming & Implementation Data	Paper copy off site storage
Emergency Services	
Disaster Preparedness & Recovery Plans	Paper copy off-site storage
Facility & Property Management	
Encroachments	Microfilm
Engineering & Architectural Drawings & Specs.	Microfilm
Key/Card Key Inventory	Paper copy off-site storage
Land Information Files	Microfilm
Operating Manuals	Paper copy off-site storage
Fire & Emergency Medical Services	
Annual Report Adopted--Fire Fighter Board of Trustees	Microfilm
Minutes of Fire Fighter Board of Trustees Proceedings	Microfilm
Governing Councils, Commissions, and Boards	
Agency Charters	Microfilm
Franchises	Microfilm

Indexes to Minutes, Ordinances, & Resolutions	Microfilm
Minutes of Official Proceedings	Microfilm
Oaths of Office	Microfilm
Ordinances & Resolutions	Microfilm
Records of Public Hearings	Microfilm

Hazardous Materials Administration
Generator Annual Dangerous Waste Report	Microfilm
Hazardous Materials Abatement Project File	Microfilm
Hazardous Material Accident/Incident Report	Microfilm
Hazardous Materials Certificate of Destruction	Microfilm
Hazardous Materials Disposal Records	Microfilm
Haz. Mat. Employee Right to Know Implementation Plan	Microfilm
Hazardous Materials Inspection & Test Reports	Microfilm
Hazardous Materials Inventory Sheet	Microfilm
Hazardous Materials Management Plan	Microfilm
Hazardous Materials Trained Personnel List	Microfilm
Materials Safety Data Sheet (MSDS)	Microfilm
Physical Exam Reports For Employees Exposed to Haz. Mat.	Microfilm

Housing Authorities
Property History Files	Paper copy off-site storage

Insurance/Risk Management/Safety
Certificates of Insurance	Microfilm
Disaster/Emergency Management Plan	Microfilm
Insurance Policies Purchased	Paper copy off-site storage

Irrigation Utilities
Herbicide & Pesticide Spray Documentation	Microfilm
Land Use History Files	Paper copy off-site storage

Juvenile Services
Daily Recordings of Juvenile Court Documents	Microfilm
Detention Log	Paper copy off-site storage
Detention Roster	Paper copy off-site storage
Dockets Court	Microfilm
Juvenile Court Case File Indexes	Microfilm
Juvenile Court Case Files	Microfilm
Medical History Files	
Social Files	Paper copy off-site storage

Land Use Planning Permits & Appeals
Administrative Appeals Case Files	Microfilm
Annexation History Files	Microfilm
Approved (Binding) Site Plans	Microfilm
Building Construction & Modification Permit Files (Valid)	Microfilm
Building Construction & Modification Permit Indexes	Microfilm
Comprehensive Land Use Plan & Amendments	Microfilm
Conditional Use Permits	Microfilm
Critical Materials List	Microfilm
Maps, Drawings, Photographs (Official)	Microfilm
Maps, Drawings, Photographs (Reference)	
Open Space Classification Case Files	Microfilm
Plat Case Files	Microfilm
SEPA Determination of Significance or Nonsignificant	Microfilm
SEPA Environmental Checklist	Microfilm

Shoreline Management Permits	Microfilm
Zoning Exceptions/Waivers	Microfilm

Library
Catalog	Paper copy off-site storage
Interlibrary Loan Documentation	Paper copy off -site storage
Shelf List /Inventory of Holdings	Paper copy off-site storage

Parks & Recreation
Design Standards Reference File	Paper copy off-site storage
Park Maps	Microfilm
Project Plans & Drawings	Microfilm

Personnel
Affirmative Action Plans	Paper copy off-site storage
Collective Bargaining Agreements	Paper copy off-site storage
Employee Benefit Contracts/Policies/Plans	Paper copy off-site storage
Emp Ben Participation/Enrollment Agreements &Withdrawals	Paper copy off-site storage
Employee History	Paper copy off-site storage
HBV & HIV Exposure Reports & Waivers	Paper copy off-site storage
Minutes of Civil Service Commission Proceedings, (A & S)	Microfilm
Volunteer Files	Paper copy off-site storage

Port Districts
Airport Certification Files	Microfilm

Public Works - Engineering
Aerial Survey Photograph Prints, Negatives & Flight Map	Paper copy off-site storage
As-Built Construction Project Plans	Microfilm
Bridge Inspection Files	Microfilm
Bridge Maintenance History Files	Microfilm
Franchise History Files	Microfilm
Franchise Working Files	Microfilm
Land Survey Field Books	Microfilm
Right -of -Way Case Files	Microfilm
Right - of -Way Vacation Files	Microfilm
Road Establishment Case Files	Paper copy off-site storage
Road Maintenance History Files	Paper copy off-site storage
Survey Maps Filed for Record	Microfilm

Records Management
Public Records Destruction Log	Paper copy off-site storage
Records Center Transmittals, Inventories, & Indexes	Paper copy off-site storage

Sewer & Water System Documentation
Grinder Pump Maintenance & Location Records	Microfilm
History Files - Sewage Treatment Plants	Microfilm
Hydrant Records	Paper copy off-site storage
Industrial Waste Permits	Paper copy off-site storage
Manhole Records	Paper copy off-site storage
Maps & Geographic Data	Microfilm
Meter Records	Paper copy off-site storage
Operations & Maintenance Manuals-Sewage Treatment Plants	Microfilm
Operations Log-Sewage Treatment Plants	Microfilm
Pipe Records	Paper copy off-site storage
Valve Records	Paper copy off-site storage

Social Services
Client Case Files (Treatment Completed & Case Closed)	Paper copy off-site storage

` Client Screening & Referral Files (Completed & Closed)	Paper copy off-site storage
Facilities Inspections & Certifications	Paper copy off-site storage
Solid Waste Management	
Certificate of Disposal & Destruction of Hazardous Waste	Microfilm
Landfill/Transfer Station History Files	Microfilm
Landfill Site Closure & Custodial Files	Microfilm
Landfill/Transfer Station Site Testing & Monitoring Records	Paper copy off-site storage
Surface Water Drainage & Flood Control	
Flood Control Plan	Microfilm
Flood Damage Survey Reports	Paper copy off-site storage
Surface Water Management Project Plans & Specifications	Microfilm

B-4 Electronic Records Backup and Recovery

Put data processing plans here if your agency has an Information Technology Department, it probably has a disaster protection and recovery plan. If there is no IT department, or if there is no plan, you will need to develop one, even if it is for "stand alone" desk-top computers. In this section, list:

When and how routine backups are to be done, and where off-site copies are to be stored.

How to get access to off-site storage copies, including at night, on weekends, and during holidays.

Potential hot- and cold-sites you could use if data processing functions must be transferred off-site.

How equipment, software, and data files would be moved to those off-site locations.

Companies that can salvage your computer equipment, data files, etc. (see Appendix D)

The primary strategy for protecting data on small systems is similar to those developed for protecting large ones. The main defense is duplication. Data on servers and PCs should be backed up routinely, normally daily and weekly. The backup data should be stored in a safe place, off site. Programs, operating systems, and documentation should also be stored off site. Disaster team members must have access to everything.

BACKUP CONCEPTS FOR PCs AND LAPTOPS

Approach the problem of backing up computers with the assumption that important data is always at risk. It is not a question of 'if' the data will be compromised, but 'when'.

NOTE: It is far easier to back up and restore data than to attempt to salvage the media such as disks, tapes, or hard drives.

The most common scenario for data loss in personal computers is hard drive failure. Whether it is critical operating system files that become corrupt on a drive or a physical failure of a drive itself, data can often be recovered. But it will take time, effort, labor and money.

For laptop owners, a likely and threatening scenario is theft. In this situation, critical data is gone forever, with little hope of any recovery.

Other causes for data loss include:
- Failure due to environmental hazards like power surges, spikes, electrostatic shocks and heat
- Negligent or unauthorized users such as small children

- Malicious code, viruses, hacker intrusions

Backing up data is not a difficult task. For most people, identifying which data to back up can be the most challenging part. Figuring out where to place the backup data can also be challenging. However, once a process is identified, backing up data can be a simple routine that is easy to schedule or even automate.

Data
- Define the information to be backed up
  - Critical data that cannot be reproduced
  - Operating systems or applications can usually be reinstalled from separate source media. These are not good candidates to backup.
  - Applications, setup files and source code that only reside on the hard drive should be backed up.
  - Documents, database, web content, images and any other files that are considered important

- Consolidate/organize data in a way that is manageable
  - Data should be organized in a way that makes sense to the user
  - Consolidate backup data up under a source directory
    - 'My Documents' is an example for Windows users
    - Data can be consolidated under a user profile if multiple users access the system
    - If applicable, identify other ways that data can be organized within subfolders.
      - Dates – Useful for financial records
      - Type of content – Images
      - Subject – Documents, projects, etc…

The reason for organizing and consolidating data within a source directory is so that the user can quickly and easily identify a group or groups of data that should be backed up. Further organization helps the user to assign priorities, schedules and also creates logical associations for recovery purposes.

- Backup Media

If the PC or laptop is connected to a Local Area Network (LAN), the first choice of backup media is the LAN itself. This is assuming that the LAN is routinely backed up.

If not backed up to the LAN, the choice of backup media depends largely on the preference of the user. However, a few guidelines should be followed:
- Media should exist in different location than source
- Media should be easily portable.
- Media should be current with modern technology.

The user should decide what type of media he or she feels comfortable using. Power users may prefer tape drives with their large capacity, but they can be more difficult to use for an ordinary user. Zip drives and CD burners are the most prevalent forms of removable media on the market. Windows XP features drag and drop capabilities between the hard drive and CD burners, which make writing to CDs very easy. For non XP systems, the CD burning utilities are often quite easy to learn. Floppy disks should be the last choice.

The obvious limitations with such devices are size. CDs are available in 650 and 800 MB sizes. Zip drives start at 100, 250 and may now include even larger drives. If the data store is larger than the available media can hold, the user will need to further organize the data on the PC into smaller groups so that it can be copied in multiple backups.

Some people may wish to use a large capacity external hard drive, which would also work. Of course, the associated cost of these devices is somewhat higher than CDs, and they are not as interchangeable as a CD.

B-5 Risk Assessment and Prevention Procedure (Templates)

Awareness is important in disaster prevention efforts. Vigilance can often prevent a disaster or minimize the damage of a disaster. Employees can take the initiative to be troubleshooters and note problems that may be occurring in the building.

Problems such as leaky pipes, cracked windows, toilet problems, or unusual odors (particularly those that could indicate a fire) should be brought to the attention of the _____ *[specify maintenance supervisor, recovery coordinator, etc.].* Correcting a problem before it develops into a full-blown disaster can save great amounts of labor and thousands of dollars of records recovery and equipment salvage costs.

1.   The _____ *[specify personnel officer or other]* will insure that each new staff member reads a copy of the records disaster response and recovery plan. Supervisors will also read the plan and become familiar with its layout and content.

2.   The _____ *[specify recovery coordinator or other staff]* will inventory the disaster supply kit(s) _____ *[specify frequency; monthly, quarterly, annually]*, noting the supplies on hand, those needing to be refreshed, and those that would have to be purchased in case of emergency.

3.   The list of vendors and consultants in *Appendix D -- Supplies and Services,* will be updated _____ *[specify annual or more frequent updates]* by_____ *[specify recovery coordinator or other staff].*

4.   The _____ *[specify recovery coordinator or other staff]* will review the full Disaster Response and Recovery Plan _____ *[specify annual or more frequent review]*, updating sections as necessary, and distribute copies of updates to the disaster recovery team members, and designated agency staff.

5.   The _____ *[specify recovery coordinator or other staff]* will arrange for inspections using the Inspection Checklist and work with appropriate staff to ensure that problems are remedied.

B-6-1 Facility Risk Assessment Inspections

B-6-1-1 Maintenance

The _____ *[specify maintenance/facilities department or other appropriate unit]* will identify and inspect all areas and equipment that may cause or be subject to damage in a disaster. These will include areas noted in the Inspection Checklist that relate to:

> HVAC system
> Electrical appliances and wiring
> Plumbing and drainage
> Housekeeping

If possible, also state the frequency of these inspections and that copies of completed inspection reports will be submitted to the recovery coordinator.

B -6-1-2 Fire Safety

The _____ *[specify safety officer, or other appropriate unit]* will manage the fire safety program. This will include inspection and maintenance of fire protection systems and devices. Activities and inspections will include areas listed in the Inspection Checklist that relate to:

> Fire extinguishers
> Fire alarm system
> Smoke and heat detectors
> Fire suppression systems (sprinklers, halon, etc.)
> Liaison with the Fire Department
> Staff training

If possible, also state the frequency of these inspections and insure that copies of completed inspection reports will be submitted to the recovery coordinator.

B-6-1-3 Security

The _____ *[specify safety office or other appropriate unit]* will manage the security program, in conjunction with _____ *[specify records coordinator or records officer or other unit that supervises use of the records and record systems]* who oversees use of the records within the facility. This will include inspection and maintenance of security systems and devices such as sound alarms and silent alarm subscription alarm services. Activities and inspections will include areas listed within the Inspection Checklist that relate to:

> Key control
> Monitoring of security devices on doors, windows, inside and outside of the building

If possible, also state the frequency of these inspections and that copies of completed inspection reports will be submitted to the recovery coordinator.

B-6-1-4 Record Storage Areas

The _____ *[specify appropriate records coordinator or officer, manager, supervisor]* will ensure periodic inspection of records storage areas according to criteria listed in the Inspection Checklist. Inspections will give particular attention to:

> Signs of leaks, water damage, etc.
> Signs of mold, insect, or rodent infestation
> *[Add other reminders for particular threats to your records and facilities].*

Inspections will include all additional on- and off-site areas used for records storage.

If possible, also state the frequency of these inspections. Daily inspection is recommended. Also note that copies of completed inspection reports will be submitted to the recovery coordinator, if that is a different person than the records coordinator/officer, who has responsibility for inspection of the records storage areas.

B-7 Records Risk Assessment Inspection Checklist Templates

The following checklist templates can be useful in carrying out risk assessment inspections. Their use can reduce vulnerability of records to a disaster. Some of the inspections outlined in those checklists may be the duty of personnel

responsible for facilities maintenance, safety and fire prevention and not the DRT. Work with those individuals to develop a reasonable schedule for the inspections and establish mechanisms to verify that inspections are done as scheduled. Create a procedure that ensures you will be informed of remedial actions needed and taken. Retain copies of completed inspection reports here or see that the risk management officer receives and retains them.

These are part of a larger number of disaster prevention checklists designed for a comprehensive agency disaster preparedness program. The entire set is contained in the web version of this manual. You may want to review those checklists and recommend them to your agency Emergency Management office or Disaster Preparedness Committee.

Records Risk Assessment Inspection Checklist Templates

1. General Preparedness	OK?	Needs Action (Describe)	Action Complete (Date & Initial)
Records Disaster Plan written and updated			
Emergency Instructions posted at all staff phones			
Disaster supply kit(s) created and inventoried on schedule			
All shut-off valves, breaker switches, etc. properly labeled			

2. Plumbing	OK?	Needs Action (Describe)	Action Complete (Date & Initial)
Pipes and plumbing well-supported			
Pipes and plumbing free of leaks			
Staff know location of water main and have appropriate tools (if needed) for shut-off			

3. Fire Safety	OK?	Needs Action (Describe)	Action Complete (Date & Initial)
Appliance cords in good condition			
Appliances turned off and unplugged nightly			
Schedule visits with the Fire Marshal to follow-up on observed code violations			
Floor plans identifying location of essential records given to Fire Department			
Detection systems:			
appropriate type(s) present			
wired to 24-hour monitoring station			
tested regularly			
Fire extinguishers present, inspected regularly and re-charged if necessary			
Automatic suppression system (e.g., sprinklers, halon) present and operating			
Fire drill conducted twice per year			
Staff trained in:			
sounding alarms			
interpreting enunciator panels (if present)			
notifying Fire Department and others as called for			
using extinguishers			
turning off power, HVAC, sprinklers, gas main			
closing fire doors			

4. Housekeeping	OK?	Needs Action (Describe)	Action Complete (Date & Initial)
Cleaning supplies and other flammables stored safely			
Trash removed nightly			

5. Files and Records Storage Areas	OK?	Needs Action (Describe)	Action Complete (Date & Initial)
Shelves well-braced			
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			
Flashlights kept in windowless and dark areas, and batteries checked			

6. Protection from Water Damage	OK?	Needs Action (Describe)	Action Complete (Date & Initial)
No water sources located above records			
Water detectors present			
Storage areas checked daily for leaks, seepage, etc. Sump pumps and backups present where needed			
Dehumidifiers available			
No leakage/seepage through walls			
Valuable materials stored above ground level			
Valuable and fragile media stored in protective enclosures			
Staff have keys to mechanical rooms and janitorial closets			

B-8 Records Recovery Priorities

In the event of a disaster, unprotected essential records should be transferred to a safe location, or salvaged in the priority order assigned below. Also see Appendix A-5 -- Floor Plans for locations of these materials and for area-specific disasters.

Priority Materials [specify record series, file number range, item, etc.]	Location (Specify Bldg, floor, room, cabinet)	Departmental Coordinator
1)		
2)		
3)		
4)		
5)		