



ARMS
Archives & Records
Management Services

University Recordkeeping Manual

Part Twelve

DISASTER PREPAREDNESS & VITAL RECORDS

Archives and Records Management Services

June 2006

© 2001 University of Sydney

Part 12 – DISASTER PREPAREDNESS & VITAL RECORDS

Table of Contents

1. Introduction	2
2. Vital Records	2
2.1 Definition	2
2.2 Identifying Vital Records	2
2.3 Managing & Storing Vital Records	3
3. Important records	4
4. Disaster Planning	4
4.1 Identifying hazards & assessing risks	4
4.1.1 Review past disasters	4
4.1.2 Physical location & environment	4
4.1.3 Access & security	5
4.2 Preventative action	5
4.2.1 Remedial action	5
4.2.2 Implement changes	6
4.2.3 General recommendations for storage	6
4.3 Recovery	6
5. Disaster Plan	7
6. Disaster Bin	7
7. Contacts	8

UNIVERSITY RECORDKEEPING MANUAL

Part 12 – Disaster Preparedness and Vital Records

1. Introduction

Records are vital to any agency's survival and success. They provide evidence of business activities, support decision-making processes, protect entitlements and rights, ensure organisational accountability and form part of the historical and cultural resources available to our society. However, too often, agencies do not recognise records as a critical resource and do not take measures to protect them. As a result when disaster strikes agencies are often left unable to meet their obligations and, sometimes, unable to survive.¹

The purpose of this chapter is to provide guidelines on the identification, storage and protection of records vital to the University and to assist officers of the University to plan so as to minimise impact and enable business continuity in the event of a disaster.

2. Vital Records

The identification and protection of vital records is crucial to both effective records management and to the organisation as a whole.

2.1 Definition

According to the Australian Standard on Records Management, AS 4390, “*vital records* are those without which the organisation could not function.”

- They enable the organisation to continue operating during or following an emergency or disaster without a break in business continuity.
- They document procedures and processes so that damaged systems (both technical and administrative) can be repaired or re-established.
- They “establish and protect the rights and interests of the organisation and its clients”.²

2.2 Identifying Vital Records

In a generic sense, vital records are those which:

- “prove ownership of property, equipment, vehicles (and) products”.³ These include contracts and agreements.
- Record how the organisation operates by financial and tax records, and personnel records, including leave data, salary records etc
- Document procedures and policies, goals and planning.

¹ “Disaster Management for Records”, in *Government Recordkeeping Manual*, State Records Authority of New South Wales, 1999, p.6

² AS 4390 – 1996, *Records Management*, Part 6, Clause 6.1.2, p.7.

³ *Government Recordkeeping Manual, op.cit.*, p.14

In a **University context**, *vital records* include:

- Research contracts, including the administration of grants
- Student data, including academic transcripts, enrolment data, results etc
- Alumni data, The Register of Graduates
- The University By-laws
- Minutes of high-level committees where significant decision-making takes place, for example, Senate, Academic Board and Faculty Minutes
- Deeds and Certificates of title
- Building information relating to access and egress, electrical and network architecture, sewer lines etc
- Examination timetabling, accommodation, supervision etc
- Most contracts and agreements, including those of consultancies and consultants, software and hardware, licensing, intellectual property, buildings and accommodation
- Major publications while in production, Calendars, Handbooks, Annual Reports etc.
- Records of conferences being organised at and by the University
- Donor and bequest records
- Records pertaining to prizes and scholarships
- Records relating to curriculum and course development

And any other records, where their absence would severely impede the function of the whole University or part/s of the University. The *Government Recordkeeping Manual* describes these records as “irreplaceable and mission-critical”.⁴

2.3 Managing & Storing Vital Records

It is crucial that official University records identified as being *vital records* be registered into the University’s official records management system, TRIM.

Once the file is created and registered, it will either:

- (a) Be stored by Records Management Services (RMS) in their secure, fire-proof room
- (b) The original stored by RMS while a copy is provided for circulation and use, *or*
- (c) The newly created file stored in the relevant office until no longer active.

As *vital records* protect the organisation from loss or delays, they must be stored in such a way as to make them readily available for as long as they are current. Option (a) occurs where the matter is finalised, for example, the contract is signed, and the vital record can be stored for the length of its retention period before disposal. Option (b) will occur when the matter is ongoing, the file is still being heavily used, and it is deemed necessary to retain the original in a secure environment to prevent loss or damage from handling. Option (c) will occur when the file relates to a current matter but is

⁴ *ibid.*,p.15

not heavily used and there are facilities within the office to provide a secure environment. These requirements can be discussed with RMS when the file is being created.

3. Important Records

While the management of *vital records* is most critical, we also need to address the issue of *important records*. The Government Recordkeeping Manual defines *important records* as “those records which are not irreplaceable but could be reproduced only at considerable expense, time and labour”.⁵

It is not always easy to distinguish between *vital records* and *important records* and it would be wise to err in the favour of caution. When the potential cost of reproducing important records is evaluated, it would be sensible to treat them as *vital records* and thereby ensure their preservation and availability.

4. Disaster Planning

Disasters do occur. They may be small, such as power failure leading to some data loss, or large, such as fires or explosions. Although comprehensive planning and remedial action will minimise risks, it is not possible to eliminate them entirely. This section of the chapter will provide guidelines in analysing risks, taking preventative action, and planning for recovery.

4.1 Identifying hazards and assessing risks

4.1.1 Review past disasters: Have any incidents occurred in the past which put records at risk? These events might be: fires; leaks or flooding; break-ins or security breaches; electrical failure or fires; chemical spills etc. And have remedial measures been taken to prevent, wherever possible, a re-occurrence of these incidents? Always thoroughly document any incidents of this kind, including such information as: what, why and how the incident happened, what the results were and how long it took to recover.

4.1.2 Physical location and environment of the file storage area: The file storage area should be surveyed and notes made of any of the following:

- Where are the records kept?
- Are there overhead pipes which do or may leak?
- Is there any dampness, mustiness or mould in the area which may indicate rising damp or leaks in the wall cavity?
- Can the area be securely locked?

⁵ *loc.cit.*

- Are the doors fire-rated?
- Is there any evidence of insect or vermin infestations?
- What are the temperature and humidity levels? Are they fairly constant or are there wide fluctuations?
- Is there prolonged sunlight in the records area?
- What kind of fire suppression systems are in place? If water-based, are they directly overhead the storage area?
- Are inflammable chemicals stored nearby?
- Are the building's drains unblocked regularly?

4.1.3 Access and security:

Information relating to access and security should also be noted on the survey form.

- Who has access to the area?
- Can the records be locked away when the room is unattended?
- Who has access to computerised data?
- Is the access route to records storage clear and unimpeded by stores, boxes etc?
- Where are the exits and evacuation points?
- What is the security in the buildings? Are there alarms, keycard access, after hour access?
- Are the emergency and evacuation procedures tested regularly?

4.2 Preventative action

Once you have conducted your survey and identified potential risks, then proceed to take remedial action where possible. If a risk cannot be removed or minimised, you may need to move the records, or store them in a different way.

4.2.1 Remedial action

Where a problem can be remedied, take steps to do so. This might include:

- Repairing plumbing leaks
- Arranging for gutters to be cleared of leaves and debris
- Getting the pest exterminators in (check what chemicals are used)
- Clear access to the files, removing rubbish
- Using proper electrical hardware, don't piggy-back plugs, use heaters with exposed elements or drape electrical cords across walkways
- Keeping blinds lowered in areas with strong sunlight
- Removing stores of inflammable chemicals from the area
- Increasing security, lock the storeroom door or filing cabinet when the room is unsupervised
- Locking the computer when not in use
- Arranging for foam fire suppressant systems rather than water
- For open shelf systems, raising the bottom shelf above potential water level or don't use the bottom shelf at all.

4.2.2 Implement changes

When it is not possible to remedy an existing problem, it may be necessary to implement changes to the records storage situation.

These changes might include:

- Moving the records to another, better location
- Changing the storage system, eg. place into a locked cupboard when there is no other security
- Arranging for air conditioning to be installed to regulate temperature
- Install a de-humidifier in very humid areas
- Place files into archive boxes to eliminate dust and light and slow the affect of water or smoke in the event of a fire
- Store away from direct sunlight

4.2.3 General recommendations for storing vital records

- Always keep a copy or back-up at a different location
- Always keep record/file lists up-to-date
- Make the file list available to all relevant personnel in the event that the person managing the records is unavailable when a disaster takes place
- Keep all vital records together in case they have to be evacuated from the building
- Make sure that all relevant personnel have a copy of a current disaster preparedness plan and that a spare copy is stored off-site so that it is available when access to the building is not permitted or possible.

4.3 Recovery

The recovery “phase is that of establishing and carrying out a program to restore to a stable and usable condition both the disaster site and the damaged materials”.⁶

Should a disaster occur, you will wish to resume normal business as quickly as possible. Usually little can be done until the emergency services personnel (should they be involved) have finished their work and access is permitted back into the building. However, you can prepare yourselves for the next step, that is, the recovery of the records and re-establishment of working systems. If you have taken the remedial and preventative action detailed above, recovery should not, in most circumstances, be that difficult. You will have identified the *vital records*, either hard copy or electronic, and they will be backed up off-site, your records will be protected from the worst of water or smoke damage, and you will have a disaster preparedness plan in place to which to refer.

The first action you should take is to rally the relevant personnel (nominated in the Plan) and resources required to recover full operational capability.

⁶ Ross Harvey, ' Preservation', in Judith Ellis(ed.), *Keeping Archives*, 2nd Edition, Thorpe in Association with The Australian Society of Archivists Inc., 1993,p.101.

Resources will include services, such as drying facilities, temporary storage, and equipment and supplies.

5. Disaster Plan

No.	Task	Action required
1.	Define roles and responsibilities	(a) Nominate coordinator, backup coordinator and committee (if required) (b) Allocate specific roles (c) Develop contact list
2.	Identify vital records	(a) Conduct survey, according to criteria in Section 2 (b) Liaise with RMS re file creation, storage etc.
3.	Identify and document risks	According to Section 4.1
4.	Undertake remedial and preventative action	According to Section 4.2
5.	Identify temporary storage site (in case of need to evacuate records)	Liaise with Facilities Management, colleagues in other offices. Perhaps offer complementary facilities in return.
6.	Develop list of emergency contacts	List Police, Fire brigade, Ambulance, plumbers, electricians, Risk Management, specialists in disaster recovery services
7.	Prepare a disaster bin	Purchase some supplies to use in the event of 'small' disasters, such as leaks or the dust from building activity (see below)
8.	Draw up a one page 'action plan'	The plan should have emergency contact numbers and a simple step-by-step list of actions to take in the event of an emergency. Every staff member in the area should have a copy of this sheet at their work place.

6. Disaster bin

A disaster bin should be mobile, such as a wheelie bin or crate with handles. The bin should contain:

- paper towels
- dusters
- garbage bags
- plastic sheeting
- mops and large sponges

- packing tape
- felt tip pens
- protective gloves
- buckets
- scissors
- string
- first aid kit
- Writing pads and pens for listing.
- fan for drying
- Also, if possible, obtain a wet and dry vacuum cleaner for clean-ups.

The supplies can be shared between neighbouring offices. Always ensure that the bin is readily accessible. It will be no use to you behind a locked door.

For further information please contact the ARMS team at the numbers below.

7. Contacts

Tim Robinson

Manager, Archives and Records Management Services
 Archives, Records, FOI and Privacy
 Telephone: (02) 9351 4263
 Facsimile: (02) 9351 7304
 E-Mail: Tim.robinson@staff.usyd.edu.au

Anne Picot

Assistant Manager, Archives and Records Management Services
 Archives, FOI and Privacy
 Telephone: (02) 9351 7262
 Facsimile: (02) 9351 7304
 E-mail: Anne.Picot@staff.usyd.edu.au

Jane Tyrrell

Acting Records Manager
 Records Management Services
 Telephone: (02) 9351 2037
 Facsimile: (02) 9351 4173
 E-mail: jtyrrell@usyd.edu.au