Information Management Advice 26 Disaster Preparedness and Recovery

Introduction

The purpose of this Advice is to provide guidance in relation to your agency's preparedness for, and recovery from natural and man-made disasters.

This Advice describes the process for drawing up a Disaster Preparedness Plan for protecting and recovering records held by your agency. In particular it enables agencies to assess and prioritise what are their vital records and based on this create a plan that can be easily reviewed and updated.

The Disaster Preparedness Plan should complement and be integrated with other emergency plans relevant to your agency. In particular, most agencies will have plans authorised for dealing with building security, fire precautions, fire extinguishing systems, electricity, gas, water, chemical hazards, structural requirements, first aid and data protection.

Standards in Disaster Preparedness

In 1996 Standards Australia released *Australian Standard AS 4390-1996: Records Management*. This Standard sets out the responsibilities and strategies of high-quality records management systems, including action relating to disaster management and preparedness. Standards Australia has since released *Handbook HB221:2004 Business Continuity Management and Handbook HB292:2006 A Practitioners Guide to Business Continuity Management*, both of which are also recommended reading.

Disasters and Records

There are a variety of definitions for disasters with some distinguishing disasters from emergencies. The definition of a minor disaster is 'that although affected, the agency is still able to open for business.' The definition of a major disaster is 'an event that makes it necessary for the agency to cease operation while the situation is rectified'.

Disasters affecting records may include:

- natural events or hazards including bushfires, floods, vermin, lightning strikes, windstorms
- structural or building failure such as malfunctioning sprinklers, heating or air conditioning systems, leaks in roofs, poor wiring, sewer/ stormwater/ drainage failure, energy failure
- industrial accidents such as nuclear or chemical spills, fire, explosions, gas leaks, falling object damage
- technological disasters such as viruses and computer equipment failures
- criminal behaviour such as theft, arson, espionage, vandalism, bombing, demonstrations and terrorism
- accidental loss through human error

Disasters may also be caused by storage conditions that are unsuitable for the media stored, and by the natural decay of materials.

Stage 1 - Assessment

The identification and assessment of risk is the first stage in developing effective counter disaster management strategies for your agency's records and recordkeeping systems.

The recommended methodology is based on the *Australian/New Zealand Standard AS 4360-1999, Risk Management* and involves the following:

- Establish the context. In other words, what is the scope that the assessment needs to cover (eg. multiple or single work sites, mix of mobile or desk based staff, etc.)
- Identify the risks to records and recordkeeping systems. Agencies need to identify what are vital records (see Stage 2) to your agency and what equipment would be required in order to continue operations. If the recovery lead-time for replacing an electronic record is unacceptable then a backup alternative is usually considered.
- Analyse the risks in terms of probability and effect. In other words, which disasters are more likely to be a risk for your agency.
- Assess the risks in terms of acceptability and priorities for treatment. In other words, assess which disasters are so unlikely that to prepare for their eventuality cannot be justified. (For more on treatment priorities and vital records see Stage 2)
- Treat the risks by identifying, evaluating and implementing options. This involves developing and implementing a disaster preparedness plan (see Stage 3)
- Monitoring and review

Stage 2 - Priorities

Based on your assessment, priorities can now be determined.

Vital records are those deemed essential to reconstruct and continue operations of the agency and to protect its organisational, legal and financial interests.

Only a small proportion of an agency's records are vital records. Most permanent records identified under an approved Retention and Disposal Schedule are vital records. However, a vital record is not necessarily one with long-term value; it may only have short term value. Other vital records may include:

- the agency's disaster preparedness plan
- employee details, including contact information and payroll details
- delegations of authority
- current customer and stakeholder records or registers
- contracts, titles, and other signed original legal records
- licences, leases, permits which enable the public authority to operate or perform a particular action
- insurance records
- financial information e.g. current or unaudited accounting and tax records
- infrastructure plans, operational policies and procedures
- records relating to current or potential litigation
- other record types depending on the core business of your agency

It is essential that your agency's computer system programs are backed up on a regular basis. Your IT section should be able to provide you with its back-up schedule for inclusion in your plan. However, if your IT section is not on site it may not be necessary to include this information in detail in your plan. For more information on backups please refer to our *Advice 25 Management of backups.*

As part of vital records protection and recovery, data critical to the reconstitution of your agency's electronic records should be identified and able to be restored easily. Without the recovery and restoration of this data, business processes involving electronic recordkeeping may be impossible to recover and restore.

Measures for protecting and recovering data critical to the reconstitution of electronic records should be integrated with arrangements for protecting your agency's vital records. Critical data recovery planning ensures that copies of electronic datasets and their most current updates (whether in electronic form or as paper based input documents) are:

- available to the recovery effort
- not destroyed by the same disaster event that renders the workplace and business operations untenable
- stored in a safe location, preferably off-site, and
- able to be restored within a specific timeframe to an accessible form for processing by systems, networks, and end users.

Stage 3 - The Disaster Preparedness Plan

Writers on counter disaster planning usually advocate one of two approaches:

- minimalist planning so that the plan is easily updateable and less resource intensive so that response is facilitated
- detailed plans containing information on how to respond to the major disasters for each of your agency's record formats

The level of detail will depend on the resources and time available for the development of the plan. It is important to plan for the most likely disasters identified at the Assessment stage. For example, agencies can reasonably expect to treat the effects of fire and water. However, in a disaster, staff will be under pressure so the plans should be as concise and easy to follow as possible.

The basic components of the plan may vary according to organisational needs, but should include the following:

- a list of vital records, particularly significant or vulnerable holdings, and location and control documentation
- the function, composition and chain of command of the emergency response team(s) and their contact information (see stage 4)
- a list of equipment and materials available for use in disaster salvage and recovery (see Appendix 1)
- procedures for identification and declaration of a disaster situation and initiation of the disaster response chain of command
- provisions for the training and current awareness of the emergency response team(s)
- a list of sources of back-up resources, including expertise, trades people, materials, equipment, vehicles and accommodation
- procedures for updating and testing the disaster preparedness plan

- simple technical information on the handling of damaged material which directs the user to what are priorities for early treatment.

A clearly written counter disaster plan is much easier to maintain, implement and use. Tips in writing include:

- write the plan with the assumption it may be implemented by personnel unfamiliar with the operations of your agency
- use direct language with short paragraphs
- present one idea at a time
- use a standard format that avoids jargon
- use position titles (rather than personal names) to reduce maintenance and revision requirements
- develop uniformity in procedures to simplify the training process and minimise exceptions to conditions and actions
- identify events that occur in parallel, and events that must occur sequentially
- interlink with supporting documentation (e.g. checklists)

The plan needs to be regularly tested and maintained in order to be relevant. It should be reviewed and improved regularly to reflect your agency's current operating environment, for example when there are:

- changes to personnel assigned responsibilities within the plan
- changes in procedures
- new vital records
- new equipment or systems
- new building locations or changes to building structures
- changes to standards or best practice.

The plan should be tested periodically to maintain awareness, and to reveal any flaws. Supplies in disaster bins and rooms also need to be checked regularly to ensure that they have not been tampered with or depleted. Formal responsibility for the review should be assigned.

Reviews should be conducted after testing and after emergency situations to consider successes and failures and how implementation procedures might be changed to work more effectively. Internal audits of the counter disaster plan may also be conducted on at least a yearly basis. Changes to the plan should be documented to show the history of plan development. Agencies may also consider having their plan externally audited by a disaster management service provider.

Stage 4 - Emergency Response team(s)

After establishing the Disaster Preparedness Plan, your agency should establish a team or teams of volunteer staff from each section of the agency to take part in salvaging records. All response team members must be accessible by telephone for after-hours call-out.

Each team must have a leader and deputy and include management, technical, administrative and operational staff. Teams will need to be trained in response and recovery techniques and have good knowledge of preventive measures. Teams will need to meet at least once a year and be informed of changes in the Disaster Preparedness Plan.

Stage 5 - Response and Recovery

The Emergency Response Team should also consider what initial action the agency should take when a disaster occurs, who should be called and in what order, and what further action is required. The Tasmanian Archive and Heritage Office should be on your list of priority contacts (see our contact details on p6). Remember that your priorities in responding and recovering records affected by the disaster have been laid down in your Disaster Preparedness Plan.

Simulations and brainstorming sessions should also be used to consider the action needed to ensure that recovery is facilitated. These include, for example, damage assessment strategies, alternative sites for resuming business operations, vendor assistance, alternative sites for recovery operations, and the use of vital record duplicates.

Reporting is a significant component of the response to a disaster. You should try to keep an adequate record of the emergency so that improvements can be made to prevent similar emergencies occurring in the future, or to make the response to any subsequent ones more efficient.

Compliance Checklist

1	**Assessment**	
1.1	Has a risk assessment of potential disaster events identifying threats to records and recordkeeping systems been performed?	Yes/No
2	**Priorities**	
2.1	Have priorities been established, identifying your agency's vital records?	Yes/No
3	**Plan**	
3.1	Has a disaster preparedness plan for records and recordkeeping systems been developed and implemented	Yes/No
4	**Teams**	
4.1	Has emergency response team(s) been appointed	Yes/No
5	**Response and Recovery**	
5.1	Has the emergency response team(s) made adequate preparation for the agency's response and recovery to a disaster event?	Yes/No

Further Advice

For more detailed advice please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

‘Disaster Preparedness Manual for Commonwealth Agencies’ (National Archives of Australia 2000)

‘Disaster preparedness and recovery’ (Queensland State Archives website)

‘Standard on counter disaster strategies for records and recordkeeping systems’ (NSW State Records website)

‘Records Management Disaster Planning’ (Guideline of State Records of South Australia 2007)

Australian Standard AS 4390-1996: Records Management (Standards Australia 1996)

Handbook HB221:2004 Business Continuity Management (Standards Australia 2004)

Handbook HB292:2006 A Practitioners Guide to Business Continuity Management (Standards Australia 2006)
List of sources with links as appropriate.

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.1	April 2017	Sally Murdoch	Removed former staff contact details	Stage 5 Response and Recovery
2.0	March 2015	Christine Woods	Template	All
1.0	13-06-2012	TAHO	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template

Issued: June 2012

Ross Latham
State Archivist

Appendix 1 - Equipment and materials

To ensure efficient recovery of physical records it is essential that you have appropriate equipment and materials readily available. The following items should be purchased for a disaster kit and be easily accessible to the emergency response team(s):

- paper towels
- mops, buckets
- blank newsprint
- roll of polyethylene plastic
- sponges
- freezer paper
- plastic garbage bins
- extension cords
- labels
- paper, pencils
- plastic bin liners
- rubber gloves
- scissors, tape
- plastic string, pegs
- pliers
- torches
- clipboards
- plastic tubing
- electric fans
- absorbent cloths
- plastic paper clips
- surgical type gloves