Information Management Advice 52 Identifying and Managing Vital Records

Introduction

Business continuity and disaster preparedness depend on vital records for their success. Identifying and securing vital records across all formats is a critical aspect of risk mitigation and effective business continuity planning within an agency.

What are vital records?

Vital records are those records:

- without which agencies could not continue to operate
- are irreplaceable, or
- would require significant resources to recreate.

They contain information essential to effectively restore the agency's business operations during, or following an exceptional event (e.g. network failure, a disaster). Vital records protect the assets and interests of an agency, its clients and stakeholders, and are usually associated with the organisation's infrastructure, legal and financial matters. Generally these records require significant resources (e.g. time, money) to reconstruct if lost or damaged, or may be impossible to recreate altogether.

Vital records typically contain information critical to:

- emergency preparation and response
- core business operations (i.e. critical client services)
- protecting the legal and financial rights of the agency
- protecting the legal and financial rights of agency clients

Other vital records may include:

- the agency's disaster management or business continuity plan (which should include a vital records recovery plan)
- employee details, including contact information and payroll details
- delegations of authority
- current customer and stakeholder records or registers
- current (active) contracts, titles, and other signed original legal records such as grant deeds, partnerships or memorandums of understanding.
- current (active) licences, leases, permits which enable the agency 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 matters

Vital records are those considered critical to returning an agency to core business functionality. Vital records may be considered vital only in the short term, or may retain this status indefinitely. They may be in any format (e.g. hardcopy, microfilm, electronic, maps or plans, etc) and can have any records security classification associated.

Vital records may:

- be temporary or permanent
- exist in any format (e.g. hard copy, electronic, audio-visual tapes, microfiche, etc.)
- be found throughout an organisation.

This type of record is commonly considered to range between 5-10% of the total record holdings of an agency.

Identifying vital records

Establishing those records considered vital to an agency should be part of a broader analysis of the agency's recordkeeping requirements. Utilising risk management principles when assessing state records may help to distinguish between:

- vital records - those which are critical to operations and may be extremely difficult to replace, or incur a significant cost to reproduce
- important records - those which could be recreated with some level of resources
- useful records - those which would cause some inconvenience if lost but are replaceable
- non-essential records - those which would not cause any impact to operations if lost (e.g. records relating to the publicising of past events or services organised by the agency or records due for disposal under an approved Retention and Disposal Schedule).

A number of approaches can be used to identify those records considered vital for restoring critical business functions. These might include:

- review of the disaster management or business continuity plan for activities, and the related records needed during or following an exceptional event
- review of risk assessments
- examination of organisational structures, policies and procedures
- consultation with business managers and legal advisors
- review of the agency's statutory and regulatory responsibilities
- consideration of business activities and related records included in an agency business classification scheme, and/or an approved Retention and Disposal Schedule.

When determining that a given records series is 'vital', the agency or its records manager must be able to clearly state which mission critical operations would be prevented by the loss, destruction, or other unavailability of the indicated records series. For example, all agencies must pay their employees, withhold payroll taxes, account for pensions and other benefits. Similarly, they must maintain office buildings, warehouses or other facilities they own or occupy. Local government must maintain public safety, issue building permits, enforce building codes, and process zoning applications.

Once an agency's mission critical operations have been determined, then records essential to those operations must be identified. Make a list of the vital records in your office. It is the responsibility of each agency to analyse its own operations and associated records to determine what information is vital to its continued existence. Following are questions which can be asked to assist in identifying records vital to your operation:

- Which business processes are critical to the function of the agency? To the community?
- What records are absolutely necessary to resume operations?
- What records are necessary to protect legal and financial status of the agency, and preserve rights and obligations of employees, customers, and citizens?
- What other sources, if any, inside or outside the organization, can records be retrieved from?
- In what medium does the needed information reside – paper? electronic? microfilm? other?
- Where are the vital records located – secure offsite storage? In-house storage vault? Basement/attic? On your desk? Within business systems?

When identifying vital records, remember:

- to assess all the agency's records, regardless of location and format
- not all important records may be considered 'vital' to the agency's recovery of core business operations
- vital records should be easily accessible, up-to-date, and identified as critical to the recovery of business operations.

Establishing a Vital Records Program

It is the responsibility of agency heads to protect vital records. The Records and Information Manager is usually assigned the responsibility of developing, implementing, maintaining, and updating the Vital Records program for the agency.

A Vital Records program should be established within each agency's counter disaster plan. The program includes the policies, plans and procedures developed and implemented, and the resources needed to identify, use, and protect vital records.

In very large agencies, more than one individual may be assigned responsibility for ensuring that the Vital Records program is consistent with the overall objectives and requirements set by the organization. This should include establishing communication with the agency's Emergency Management team (or Risk Managers) to inform them of the location of vital records and the procedures for their access and recovery. Often, the development of a Vital Records program is done in conjunction with the development of a Records Management program, beginning with an inventory of the records.

There are many steps in developing a Vital Records program, but once established, the program should include the following:

- A list of all business critical processes, the systems they reside in, and associated records identified as essential to protect legal and financial status, preserve rights and obligations of employees, customers, citizens, and to ensure continuity of business operations
- Procedures to be followed to protect records, and maps or floor plans showing the location of vital records
- Procedures to create backups
- Procedures to retrieve backups in an emergency

- Procedures for the recovery and restoration of records and information after a disaster

The Vital Records program should be reviewed annually and revised/updated to reflect changes in the plan, or to the status of the records, as they occur.

Agencies should adopt a risk - based approach and consult their records manager to develop appropriate management strategies for addressing all recordkeeping concerns.

Managing vital records

Once identified, vital records should be registered. A vital records identifier/locator checklist is provided in Appendix 1. Agencies can use this checklist to identify their vital records and their whereabouts, and then develop a register from this list. A sample vital records register template is available in Appendix 2 for this purpose. Both tools are intended as starting points only, and agencies are reminded that there will be additional records specific to their business that must be identified. When registering vital records, the following details should be included for each record:

- type (e.g. brief description of record type)
- the name of the area responsible for the record service or electronic recordkeeping system containing the vital records
- explanation (e.g. brief explanation of why it is considered vital, the record's critical purpose, consequences of loss)
- location and storage (e.g. on-site, off-site, of original, of duplicate, server, data centre, backups, mirror sites, etc.)
- date for review / update / disposal
- format (e.g. hard copy, digital, audio-visual tape, etc.)
- accessibility requirements (e.g. position, authorisation, access to storage if off-site, recovery protocols for systems, etc.).

Once an agency's vital records have been identified and registered, a vital records plan should be developed, implemented and regularly reviewed. The vital records plan should be included with the agency's disaster management or business continuity plan.

There are a variety of measures agencies may employ to protect vital records, including storing records:

- on-site using data backups, a fire / flood-proof safe or storage area
- off-site in a data centre or storage facility with a high level of hazard protection (e.g. against fire, theft, flood, power failure, etc.)
- across a variety of secure secondary locations.

Protecting vital records should cover both measures to prevent or minimise the impact of a disaster event, and recovery and restoration measures if a disaster does occur.

Preventative Measures

There are a number of possible preventative strategies and each should be evaluated to ensure that it is viable and cost effective for the agency. Agencies may choose to use a range of strategies depending upon the types of record formats that they need to protect. For example, it may be feasible to store vital paper records in a fireproof safe within a storage facility that has high levels of fire and security protection.

Specific protection strategies for vital records may include:

- Duplication and dispersal
- Ensuring high levels of fire and security protection in storage containers and spaces, i.e. on-site and off-site storage
- Establishing procedures for managing critical work in progress which may not be backed up or is located outside of storage facilities.

Duplication and dispersal means creating duplicate copies of records and storing these in secondary locations. If the agency is duplicating records, such as board papers, it may be economical to duplicate the original medium to the same medium (e.g. paper to paper, microfilm to microfilm), but considerations like the stability of the media and the cost of reproduction need to be taken into account. To maximise the cost benefit, agencies may wish to reproduce to another medium, such as scanning and maintaining an electronic version, which can be used for other purposes besides protection. The costs of duplication, whether duplicates have the same legal value as the original (which version becomes the 'official' record, and which is simply a 'copy'), and appropriate disposal protocols longer term also need to be considered.

When storing duplicates at another location, such as a branch of the organisation or a commercial storage facility, the agency must ensure that the duplicates are secure and accessible only to authorised persons. See *State Records Guideline 13 Certification for Secondary Storage Providers* for further information. Dispersal should be regular, the storage location and conditions should afford adequate protection, and housings should be appropriate for the media. Any special equipment required to read vital records should also be stored at the dispersal location or alternative sources of this equipment listed in the counter disaster plan. An appropriate disposal strategy for duplicated records no longer determined to be of 'vital records' status (eg expired contracts) should be developed and systematically executed.

On-site storage involves housing vital records in fire resistant housings or file rooms (vaults) with appropriate suppression systems and security. However, records may still be vulnerable if the site suffers damage.

If storing vital records off-site, the facility should be in a safe location at sufficient distance from the main office to be unaffected by the same disasters but close enough for the convenient delivery of records. Records should be housed appropriately, and locatable when required. (See *State Records Guideline 11 Physical Storage of State Records* for more information).

The most effective approach for electronic media, is to duplicate and store duplicates in secure off-site storage. The production of backup copies of essential files should be a routine operating procedure. Backup schedules and procedures appropriate to storage, media and format should be established and rigidly enforced and audited, and responsibilities should be assigned to appropriate employees.

There are various backup methods and these should be discussed with information technology specialists. For vital records protection, backups are typically made on media that can be removed and stored offsite. Those offsite storage facilities used should have storage suitable for electronic records. Although backup schedules are recommended, they are not a comprehensive disaster prevention strategy. Preventative measures should also extend to critical work in progress that may not be backed up every day or is sitting on desks. It is important to identify and prioritise critical work in progress and then establish procedures, such as a 'clean desk policy' or additional safety measures to reduce exposure.

Recovery and Restoration

To facilitate systematic vital records recovery, the vital records recovery plan (i.e. the list of all vital records, their locations, and the procedures for the recovery of these records) should be included in the counter

disaster plan for records and recordkeeping systems. The listing of all vital records should include the location of buildings and room locations, and floor plans. The list should also include safe and vault combinations, and location of keys to all cabinets or desks or containers that house vital records, all services (power, water etc.) and where they can be shut off in an emergency; evacuation routes for staff (and for records if necessary), and the location of emergency equipment. The vital recovery procedures should be written in a clear and concise language, easily understandable by non-technical staff. Backup copies of the vital records recovery plan should be stored off-site.

The vital records recovery strategy is founded on a detailed knowledge of the organisation's records holdings including every storage area in use, its contents and their nature, the location of vital records, and the level of information contained in finding aids or indexes.

Vital records must be prioritised for recovery and restoration purposes. Remember, there should be copies of the vital records recovery plan in the organisation's counter disaster plan. (See TAHO *Advice 26 Disaster Preparedness and Recovery* for more information).

Some tips to consider:

- **Ensure storage is suitable for the record format**. Consider the location of off-site storage to ensure it is a sufficient distance from the business to not be affected by the same disaster, but still within reasonable distance for accessibility.
- **Ensure format is fit for purpose**. If your vital records are in a technology dependent medium, you need to make sure that the technology is preserved, as well as the records themselves, e.g. if you hold vital records in microfilm/microfiche you'll also need a reader to access the records. It may be prudent to ensure vital records are included in any obsolescence monitoring undertaken, and migrate accordingly.
- **Organise procedures to access and retrieve vital records in an emergency**. These should be incorporated into your counter disaster plan. Make sure you have lists and indexes that indicate what records there are, and exactly where they are (systems, and physical locations such as buildings, safes, etc)
- **Organise back up procedures for electronic vital records**. Check vital electronic records are being backed up regularly in an accessible and write protected format.
- **Develop plans**. Develop a Vital Records management plan that is viable and effective for the organisation, and applicable to all types and formats of vital records. Ensure this is included in the agency's counter disaster plan (or equivalent).
- **Allocate responsibility**. Make sure that the officers designated in the counter disaster plan are authorised to retrieve records (including security rated material), able to access storage areas (with keys, key cards, entry codes, emergency overrides or knowledge of release switches), and able to use any equipment which is required to retrieve records (computers, microfilm equipment, ladders, trolleys, forklifts).
- **Schedule regular audits**. Regularly audit vital records to ensure currency and validity, and to ensure appropriate disposal in line with an approved Retention and Disposal Schedule.
- **Undertake reviews**. Reviews should be scheduled to determine whether vital records are adequately protected, current and accessible to staff who require them. This step is particularly important if functions and activities change significantly or if compliance to the program is wavering. Periodic testing can be part of the process of testing emergency plans.

Checklist
Step 1. Review your Agency Information Asset Register and critical applications list and identify Vital Records
Step 2. Review Agency Business Classification Scheme to identify Vital Records
Step 3. Use Vital Records locator to assist you in identifying Vital Records in other formats/locations
Step 4. Draft list
Step 5. Interview Business unit Managers to identify/confirm record status as Vital Records
Step 6. Confirm responsible business owners
Step 7. Draft register document
Step 8. Develop Vital Records program management plan, including any relevant policies and procedures (eg disposal strategies, etc)
Step 9. Develop salvage and recovery strategy. Include in counter disaster plan.
Step 10. Schedule annual reviews of Vital Records program; individual record status; any incidents; and disaster recovery plan

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

- Queensland State Archives Public Records Brief Identifying and Managing Vital Records
- Archives Advice No. 12 Identifying and Protecting Vital Records Considerations for Government Officials, Georgia Archives
- State Records New South Wales - Australia
- Charles Sturt University Vital Records Policy - Australia
- Council of State Archivists – United States of America
- National Archives and Records Administration – United States of America

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
2.0	April 2015	Christine Woods	Template	All
1.0	March 2014	Allegra Huxtable	Initial Release	All

Amendments in this Release

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

Issued: March 2014

Ross Latham
State Archivist

Appendix 1 – Example of a vital records register

ID	Type	Area responsible	location	Business Owner	Controlling System (digital records)	Format	Why vital?	Risks	Protection measures	Recover if backups are suitable*	Disposal Schedule / class
1	General ledger	Finance Department	Level 2 West		Financial system	Digital	Records expenditure and revenue. Loss would cause difficulty in meeting audit responsibilities.	Data corruption Fire Fraud Hackers Viruses	Completed back-ups daily Store Back ups off-site	No	DA2200 12.01.01
2	Records registry	Records Department	Level 2 East		TRIM / RecFind / Objective / ECM etc	Digital	Control system which allows access to organisation's records and contains information showing integrity, authenticity and reliability of records. Required as State archives.	Data Corruption Fire Fraud Viruses Hackers	Completed daily back-ups Store Back ups off-site File Creation Forms Virus checkers	Yes	
3	Title deeds	Legal Services Department	Level 2 West		TRIM / RecFind / Objective / ECM etc	Digital / Paper	Shows ownership of Council owned properties. Loss would make ownership difficult to prove.	Loss of deeds	Photocopy and store offsite Store in fire proof safe	Yes	
4	Rates books	Customer Service Department	Level 1, 1990-present Level 2 East, 1870-1990		TRIM / RecFind / Objective / ECM etc Financial system	Books	Supports rights of rate payers and Council regarding rates collected. Loss would cause difficulty in proving who has paid and may cause financial hardship. Required as State archives.	Fire Fraud Virus Hackers	Microfilm books and store offsite Back up database nightly and store offsite	Yes	

5	Records regarding maintenance and conservation work on buildings of heritage value	Records Department	Level 2 North		TRIM / RecFind / Objective / ECM etc Financial system Electronic database of plans	Paper	Important for: ensuring building is maintained according to heritage standards; history of locality. Required as State archives	Fire Fraud Virus Hackers	Photocopy files and store offsite Store in fire proof safe Back up database nightly and store offsite	Yes	
6	Signed originals of Contracts (Partnership Agreements, Grant Deeds, MOUs)	Planning Department	Level 1 West		TRIM / RecFind / Objective / ECM etc	Paper			Store in fire proof safe	Yes	

Appendix 2 - Checklist: Vital Records Identifier/locator

Audit date: _____

Examples of Vital Records	**Location**
Insurance policies & schedules (original signed documents)	
Master sets of Minutes (Council meetings, Special Committees and council Committees)	
Internal/operational policy documents (current)	
Drawings, maps & plans	
Pay Rates	
Annual reports	
Bank Balances	
Research records (major projects, ventures)	
Share certificates	
Tax Returns	
Technical Reports	
Leases & Licences (include software licences)	
Customer & Debtor lists	
Inventory control records	
Grant Deeds	
Loan agreements and balances	
Mortgages	
Payroll registers	
Personnel Records	
Workers Rehab & Compensation records	
Certificates of incorporation, patents, trademarks, business names	
Copyrights	
Corporate seals	
Deeds & Certificates of Title	
Contracts & Agreements/MOUs/Partnership Agreements (original signed documents)	
Computer software licences/databases	
General Ledgers	
Joint Venture agreements & MOUs (original signed document)	
Acquisition/disposal contracts	

Due Diligence reports	
Legal Opinions/Advice	
Liability releases & indemnification agreements	
Guarantees	
Litigation files	
Master set of By-Laws	