Vital records are those records without which the University could not continue to operate and which "contain information essential to effectively restore business operations during or following an exceptional event (e.g. network failure, a disaster)"¹. They typically represent between 5-10% of University records.

Records can be divided into four categories of current business value:

- 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).

Vital records can be temporary records or permanent records: what makes a record vital is how critical it is to business operations right now, irrespective of what its value may be in the future. The category a given collection of records falls into can (and often does) change over time, with most vital records being active records. E.g. an agreement may be a vital record while in force, then becomes merely useful or non-essential once it expires.

Examples include records that contain information critical to:

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

**Identifying vital records**

The first step in identifying your vital records is to identify your business area’s critical business functions and mission critical operations. Which business processes are essential to the functioning of the University? Which records are absolutely essential to performing these operations on a day to day basis, without which work would come to a stop? Is the information contained in these records replicated any in other records or systems? If so, how difficult and time-consuming would it be to retrieve this information in order to resume operations?

---

¹ TAHO Advice 52: Identifying and Managing Vital Records
Creating a Vital Records Register

Once you have identified your vital records, they should be registered in a Vital Records Register. You can find a template [here](#). We are also developing a University wide Vital Records Register which you will be able to contribute to through a web form on our website. The following details should be included for each record:

- type/brief description
- series title (if applicable)
- business owner/area responsible
- explanation of why it is vital & which operations would be prevented by its loss
- location (physical records) / system (digital records)
- format
- accessibility requirements
- review/disposal date
- significant risks

Develop a Vital Records Plan

Beyond registering your vital records in a Vital Records Register, it is also important to develop a plan for protecting your vital records. This should include a risk management assessment of the various risks posed by natural disasters, industrial accidents, human error and malicious damage, and a plan for recovering vital records in the event of a disaster.

Risk Management Assessment

This should be carried out in accordance with Australian Standard 4360-1999 and University guidelines. You should assess both the likelihood and consequence of each risk on a matrix. For examples, see the matrix on the second worksheet of the Vital Records Register template.

You will need to consider:

- physical risks to storage areas for physical records
- physical risks to hardware hosting electronic records
- connectivity risks for externally hosted electronic records
- security risks to electronic records

Some of the risks to be considered include:

- Flooding of physical storage areas or server rooms (from storms, floods, burst pipes, sprinkler malfunction)
- Fire (electrical, chemical, bush fires, lightning strikes)
- Ransomware and other malicious hacking attacks
- Connection problems with externally-hosted documents and systems (e.g. in the Cloud)
- Accidental loss through human error

Prioritise the risks in terms of the acceptability of the overall risk. The next step is to consider the options for preventing or minimising those risks. It may not be possible or cost-effective to entirely prevent some risks, in which case you will need to consider strategies for minimising the likelihood and/or impact of the risk and for recovering if it does occur. Some examples of preventative measures include relocating records stored in risky storage areas, engineering solutions to reduce or eliminate hazards or protect records, backing up electronic records, creating access copies of records and storing the originals in a secure off-site location, and instituting procedures to minimise risks.
Disaster Recovery Plan

You will also need to either draw up a disaster recovery plan, or if one already exists, ensure that it includes a section dealing with the recovery of physical or electronic vital records that have been damaged or become temporarily inaccessible. Whether that means repairing damage, restoring access to externally hosted records or finding alternative sources for the information, the core objective is the same: to restore access to the information needed to resume operations as quickly as possible. This may require the implementation of temporary emergency measures, in which case the secondary objective is to ensure continued access to information in the medium to long term, once any emergency measures have been removed.

Further information

For more information, please visit our website at http://www.utas.edu.au/it/records. If you need help, please contact the Records Management Unit at RMU.Staff@utas.edu.au.

Related documents

- Vital Records Register template
- State Recordkeeping Advice 26: Disaster Preparedness and Recovery
- State Recordkeeping Advice 52: Identifying and Managing Vital Records
- State Recordkeeping Advice 60: Introduction to Risk Management processes
- Strategic Risk Assessment Guide

Appendix: Checklist of potential vital records

- Annual reports
- Copyrights
- Deeds and Certificates of Title
- Delegations of Authority
- General ledgers
- Grant Deeds
- Insurance policies and schedules
- Inventory control records
- Joint venture agreements, Memorandums of Understanding and contracts
- Leases
- Legal opinions
- Licenses (including software licences)
- Litigation files
- Loan agreements and balances
- Maps and floorplans
- Master set of by-laws, ordinances, statutes and resolution registers
- Master sets of committee and board minutes
- Patents and trademarks
- Pay rates and awards
- Payroll registers
- Personnel records
- Policy documents
- Share certificates
- Tax returns