Records Security Guidelines

May, 2014

Contents

1 Executive Summary .................................................................................................................. 3
2 More information .................................................................................................................... 3
3 Scope ...................................................................................................................................... 3
3.1 Application .......................................................................................................................... 3
3.2 Introduction ......................................................................................................................... 3
3.3 Risk Assessment .................................................................................................................. 3
4 Recommended Standard Procedures ....................................................................................... 4
4.1 Access Procedures .............................................................................................................. 5
4.2 Transmission Procedures ..................................................................................................... 6
4.3 Storage Procedures ............................................................................................................. 7
4.4 Procedures for Home-based or Mobile workers ................................................................. 8
4.5 Destruction Procedures ...................................................................................................... 9
5 Alternative Procedures for High Security Records ................................................................. 9
5.1 Access Procedures ............................................................................................................. 10
5.2 Transmission Procedures .................................................................................................. 10
5.3 Storage Procedures ........................................................................................................... 11
5.4 Procedures for Home-based or Mobile Workers ............................................................... 11
5.5 Destruction Procedures .................................................................................................... 12
6 Legislative Framework ........................................................................................................ 13
6.1 The Archives Act 1983 (TAS) ............................................................................................ 13
6.2 The Right to Information Act 2009 (TAS) ......................................................................... 13
6.3 The Personal Information Protection Act 2004 (TAS) ....................................................... 13
7 Glossary ................................................................................................................................... 14
8 Versioning ............................................................................................................................. 16
9 Appendix 1 – University obligations under the Archives Act 1983 (TAS) ......................... 17
<table>
<thead>
<tr>
<th><strong>Responsible Officer</strong></th>
<th>Chief Information Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved by</strong></td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td><strong>Approved and commenced</strong></td>
<td>May, 2014</td>
</tr>
<tr>
<td><strong>Review by</strong></td>
<td>May, 2017</td>
</tr>
</tbody>
</table>
| **Relevant Policy or Procedure the Guideline supports** | Records Management Policy  
Records Management Guidelines |
| **Responsible Organisational Unit** | Records Management Unit  |
Executive Summary

These Guidelines form part of the University of Tasmania ICT Security Framework. They provide procedures and directives to be followed in implementing sound practices for the security of University records as part of the Records Management Policy.

These Guidelines should be read in conjunction with the University of Tasmania ICT Security Framework, the Records Management Policy and the Records Management Guidelines, all of which are available from the UTAS Policy Repository.

More information

For further information, contact the Records Management Unit.

Email: RMU.Staff@utas.edu.au

Scope

This document applies to all records, whether paper-based or electronic, and includes information held in the TRIM corporate Electronic Document and Records Management System (EDRMS).

A record is described as “information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business”.

3.1 Application

University employees are to apply the model to all records of University business activities. In practicable terms, this requires that the employee who creates or receives the record is to apply the appropriate record security procedures.

3.2 Introduction

These Guidelines have been developed to be consistent with the Archives Act 1983 (Tas.) and AS ISO 15489 Records Management, which has been endorsed by the State Archivist as a model for best practice record keeping.

Accordingly, these Guidelines have been developed to be consistent with the Standard and in particular the section quoted below:

Development of appropriate categories of access rights and restrictions is based on the organisation's regulatory framework analysis, business activity analysis and risk assessment. Reasonable security and access will depend on both the nature and size of the organisation, as well as the content and value of the information requiring security. Reasonable security can be described as the level of security that a reasonable person on the street would believe is needed to protect the information

---

from any unauthorised access, collection, use, disclosure, deletion, alteration and/or destruction.²

These Guidelines outline a recommended minimum standard to be applied by University of Tasmania staff and provide directives to assist in assessing when appropriate changes to the minimum standard should be considered.

These Guidelines are intended to be simple to administer, using risk assessment as the basis of identifying when exceptions to normal procedures are appropriate. The features and benefits of the model include:

- The provision of standard procedures relating to information access, transmission, storage and destruction requirements for the majority of information within the University;
- The application of a risk assessment which examines the sensitivity and risks of records and then determines if an exception model is appropriate; and
- A list of alternate procedures which may be considered by staff for information warranting a higher level of security.

3.3 Risk Assessment

A core component of these Guidelines is the application of a risk assessment for all aspects of information security to determine the level of security necessary or appropriate. For the purposes of record security, staff need to identify key groups or types of records and conduct a high-level risk assessment against each. The risk assessment needs to encompass the operational responsibilities and requirements of the University.

The purpose of the assessment is to identify:

- Groups or types of records held by the University
- Whether particular groups or types of records have any particular risks or security (e.g. business, political, or legislative) requirements beyond those provided by the recommended standard procedures
- Mitigation strategies using alternate procedures to be applied to records that require higher levels of security

Groups or types of records that may require alternate procedures include those whose unauthorised access, disclosure, loss of integrity, or unavailability may:

- Seriously damage or compromise the success or adversely affect the viability of a commercial venture or law enforcement process
- Cause distress to, or threaten, an individual³

² S4.2.5.2 AS ISO 15489.2 2002 Records Management Part 2: Guidelines. A legislative test of reasonableness is also applied to the storage of personal information – refer to University Privacy Policy.
³ For example, unauthorised disclosure of sensitive student and/or staff information (including those TRIM records attracting the Student-in-Confidence or Staff-in-Confidence caveats) may cause distress to an individual staff member or student. Sensitive student information could include information relating to health, disability, disciplinary proceedings, and fee-related comments. Sensitive staff information includes any records forming part of the HR personnel file, such as information relating to health, disability, disciplinary proceedings, counselling, grievance procedures, workers compensation claims etc.
- Have specific legislative restrictions or requirements
- Cause serious financial damage to and/or lead to litigation against the University
- Cause serious loss of public confidence

4 Recommended Standard Procedures

The following procedures are recommended for use by staff as suitable for the protection of the majority of records.

It is important to note at the outset that all University records made by any staff member of the University in the course of her or his duties are considered to be confidential and must not be divulged or released to unauthorised persons without authorisation from the staff member’s supervisor or the Manager, Records and Information.

4.1 Access Procedures

Refer also to the “Access to Archived Records held at the Tasmanian Archive & Heritage Office” section in the Records Management Guidelines.

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper records should be made available to all UTAS employees and authorised third parties who have a business need to access the records.</td>
<td>Electronic records should be made available to workgroups or a clearly defined audience with a business need to access the records, with access provided to all user accounts that are members of those groups. Groups can be based on organisation structure or may include authorised third parties who have a business need to access the records. Password policy implemented on systems.</td>
<td>TRIM records should be available to all University employees with the appropriate security level assigned to their profile: Public: used for documents that are open to the public Classified: used for documents that are restricted to University employees Confidential: limits access: files and/or documents only available to authorised officers. Available to University officers having corresponding caveat (if applied) assigned to log-in. Available to University officers listed on Access Control (if applied).</td>
</tr>
</tbody>
</table>

4 For example, restrictions on access to, and disclosure of, personal information under the Personal Information Protection Act 2004 (TAS), (adopted in the University of Tasmania Privacy Policy).
5 For example, an individual may bring a complaint to the Privacy Commissioner should the University of Tasmania breach the provisions of the Personal Information Protection Act 2004 (TAS) in making an unauthorised disclosure of personal information.
4.2  Transmission Procedures

Correspondence records must clearly identify the originating section/division and show a return address in case of unsuccessful delivery.

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>No special designation when passed outside the organisation.</td>
<td>Can be transmitted across external or public networks (including the Internet) without being encrypted. The level of information contained should be assessed before transmitting. An outline of the legal responsibilities and disclaimer if received in error if content warrants application.</td>
<td>Can be transmitted across external or public networks (including the Internet) without being encrypted. The level of information contained should be assessed before transmitting. An outline of the legal responsibilities and disclaimer if received in error if content warrants application.</td>
</tr>
<tr>
<td>May be carried by internal courier service unsecured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May be carried by ordinary postal services or commercial courier firms, provided the envelope/package is sealed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 4.3 Storage Procedures

<table>
<thead>
<tr>
<th><strong>Paper Records</strong></th>
<th><strong>Electronic Records</strong></th>
<th><strong>TRIM Records</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Where possible, all records storage areas are to be secure areas with access provided only to authorised staff.</td>
<td>Use of access controls and user accounts.</td>
<td>Official documents forming part of the University's records must be captured into TRIM where the system is available to the organisational unit.</td>
</tr>
<tr>
<td>Where a secure storage area is unavailable, all University paper records should be stored in lockable cabinets, or open shelving secured by normal building security and/or door swipe card systems to prevent unauthorised access.</td>
<td>Use of appropriate controls and procedures governing applications management, maintenance, procurement, and development.</td>
<td>Storage is configured in compliance to ITS policy.</td>
</tr>
<tr>
<td></td>
<td>Management and maintenance of computer systems and networks, including disposal of associated media, should ensure appropriate integrity, availability and confidentiality of the systems and services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It should be ensured that appropriate security and contractual arrangements are in place for third party access to systems and outsourcing of system development, maintenance and/or support.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems, including University networks, should be monitored to detect deviation from the access control policy, and record monitorable evidence in case of security incidents.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information, information processing facilities and network facilities should be protected from disclosure, modification, use or theft by unauthorised persons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controls should be in place to minimise loss or damage.</td>
<td></td>
</tr>
</tbody>
</table>
ICT disaster recovery plans should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventative and recovery controls. The plans should form part of business continuity planning.

Guidelines regarding arrangements to store University Records in premises that are not owned or leased by the University are set out in the Records Management Guidelines, State Records Guideline 13 – Certification for Secondary Storage Providers and State Records Guideline 17 – Managing the Recordkeeping risks associated with Cloud Computing.

4.4 Procedures for Home-based or Mobile workers

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
</table>
| Official copies of records are not to be taken off-campus. Copies should be made for this purpose and identified as such. Where original records are required, the Manager, Records & Information should be advised prior to the records leaving the University, so they can ensure that appropriate record tracking can be undertaken and follow ups for return of files can be made. Mobile workers should ensure that official information is appropriately protected, particularly if it is sensitive. This may be achieved by:  
  - Locking paper records in an appropriate security container;  
  - Locking vehicles containing University records; | Mobile worker/home-based workers must ensure that official information is appropriately protected, particularly if it is sensitive. This can be achieved by logging off the computer or device at the conclusion of the work period. Mobile devices/iPads must be password secured and should only be used on secure wireless networks. | Access via VPN  
Mobile worker/home-based workers must ensure that official information is appropriately protected, particularly if it is sensitive. This can be achieved by logging off the computer or device at the conclusion of the work period. Mobile devices/iPads must be password secured and should only be used on secure wireless networks. |
### Paper Records
- Locking the door to their office, study or work area;
- Disposing of waste paper appropriately;
- Ensuring documents cannot be overviewed (e.g. by telephotography); or
- By a combination of these and other actions.

### Electronic Records

### TRIM Records

#### 4.5 Destruction Procedures

Records must not be destroyed unless the legal retention period specified in the relevant Retention and Disposal Schedule has elapsed or the State Archivist has authorised their destruction via a Destruction Authority.

Records authorised for destruction must be destroyed via a secure and confidential destruction method appropriate to the record format.


#### Paper Records
- Depending on the degree of confidentiality and volume of material, three methods are available to University staff:
  - Records may be placed in large containers supplied by commercial firm for security shredding;
  - Individual sheets may be passed through a paper shredder; and/or
  - Ephemeris material may be recycled by pulping or normal waste disposal processes.

#### Electronic Records
- University staff must ensure that information is wiped clean or physically destroyed, thereby avoiding possibility that only file names are deleted from the directory, ("deleted" information not being erased from the hard disc but eventually written over). Hard disks of computers and other magnetic data should be reformatted to ensure data is removed prior to computer being disposed of.

#### TRIM Records
- TRIM has built in mechanisms regarding destruction of electronic records from the data base.

#### 5 Alternative Procedures for High Security Records

Risk assessments will identify groups or types of records requiring a higher level of security than that provided by the recommended standard procedures. The following tables list some procedures staff may wish to implement should a higher level of security be required. They assume the standard procedures described above are already in place as a minimum.
5.1 Access Procedures

Limit access to permanent records transferred to the Tasmanian Archive and Heritage Office. Refer to State Records Guideline 4 – Agency Determination of Access Restrictions

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement strict controls on which University staff members are authorised to have access to the records.</td>
<td>Strict controls on membership of user groups.</td>
<td>Strict control on members of staff authorised to access files and/or documents. This may be achieved by the user by the use of one or more of the following: Assigning the &quot;Confidential&quot; security level to the record. Assigning “Caveats” to the record which limits the access to the file and/or documents by making them accessible only to authorised officers which have the same corresponding log-in. Utilising the “Access Control” mechanism. This provides additional ad hoc or group security at document and/or folder level. Users limit access to the document and related functions (akin to separate read and write access controls) to only those authorised users who must access that document in order to discharge their duties &amp;/or requirements of matter to which document relates. Full audit trail of access to information.</td>
</tr>
<tr>
<td>Audit trail of all access to information.</td>
<td>Separate read and write access controls.</td>
<td></td>
</tr>
<tr>
<td>Storage of information in separate and identified volumes or directories.</td>
<td>Storage of information in separate and identified volumes or directories.</td>
<td></td>
</tr>
</tbody>
</table>

5.2 Transmission Procedures

Accompanied by an outline of the legal responsibilities and disclaimer if received in error.

University records must be clearly marked to indicate high security procedures are required.
### 5.3 Storage Procedures

Where risk is very high, use of security guard or officer.

Provision of sealed off, fire resistant area of building for storage of computer systems and/or physical records.

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where risk is very high, use of double envelopes when posted or carried by commercial courier firms.</td>
<td>Use of encryption when transmitted across external or public networks (including the Internet).</td>
<td>Use of encryption when transmitted across external or public networks (including the Internet).</td>
</tr>
<tr>
<td>Use of sealed envelopes when carried by internal courier.</td>
<td>Where the risk is extreme, use of encryption when transmitted between University sites.</td>
<td>Where the risk is extreme, use of encryption when transmitted between University sites.</td>
</tr>
</tbody>
</table>

### 5.4 Procedures for Home-based or Mobile Workers

Records being transported are secured in locked containers.
- Mobile worker/home-based workers must ensure that official information is appropriately protected. This can be achieved by:
  - Locking information away in an appropriate security container;
  - Locking of vehicles and placing items out of sight;
  - Locking the door to the office; study or work area;
  - Disposing of waste appropriately;
  - Ensuring documents cannot be overviewed; or
  - By a combination of these and other actions.
- Mobile worker/home-based workers must ensure that sensitive official information is appropriately protected.
  - This can be achieved by logging off the computer or device at the conclusion of the work period.
  - Where the risk is very high, encryption should be used to secure the records.

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records being transported are secured in locked containers.</td>
<td>Mobile worker/home-based workers must ensure that sensitive official information is appropriately protected. This can be achieved by logging off the computer or device at the conclusion of the work period. Where the risk is very high, encryption should be used to secure the records.</td>
<td>Use of VPN to access database. Mobile worker/home-based worker to ensure that official information, particularly if it is sensitive, is appropriately protected. This may be achieved by logging off the computer at the conclusion of the work period. Where the risk is very high, encryption should be used to secure the records.</td>
</tr>
<tr>
<td>Mobile worker/home-based workers must ensure that sensitive official information is appropriately protected.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.5 **Destruction Procedures**

Records must not be destroyed unless the legal retention period specified in the relevant Retention and Disposal Schedule has elapsed or the State Archivist has authorised their destruction via a Destruction Authority.

Records authorised for destruction must be destroyed via a secure and confidential destruction method appropriate to the record format.

For detailed guidelines relating to the disposal of records see [State Records Guideline 2 - Retention and Disposal of State Records](#), [State Records Guideline 21 – Approved Destruction Methods for State Records](#) and the Records Management Guidelines.

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Records</th>
<th>TRIM Records</th>
</tr>
</thead>
</table>
| Secure destruction by shredding of the record after the time specified for retention, as determined by the State Archivist, has elapsed. | Measures which may be taken depend upon the media:  
*CDs, microfilm, microfiche* – depending upon risk, select one or a combination of: (i) physical destruction (shredding); and/or incineration.  
*Laser printer & copier drums* – depending upon risk, select one or a combination of: (i) normal disposal or recycling; (ii) sanitised by printing a quantity of non-sensitive information prior to disposal (or recycling); and/or physical destruction.  
*Magnetic media* – depending on risk, select one, or a combination of: (i) sanitised by low-level reformatting or similar activity; (ii) demagnetised and so rendered useless; and/or (iii) physical destruction.  
*PDAs, flash ROM & other emerging removable media* – depending upon risk, select one, or a combination of: (i) sanitised by low-level reformatting or similar activity; and/or physical destruction. | TRIM has built in mechanisms regarding destruction of electronic records from the database. |
6 Legislative Framework

6.1 The Archives Act 1983 (TAS)

The *Archives Act 1983 (Tas.)* is the legislation that most directly impacts on the management of records. One of the main objectives of this Act is to achieve accountability in public administration by prohibiting the unauthorised destruction or manipulation of records.

The *Archives Act 1983 (Tas.)* stipulates that records of any type may not be disposed of without the written authority of the State Archivist. Written authority may take the form of either:

- A Disposal Schedule (a continuing disposal authority listing records by type and identifying appropriate disposal actions); or
- An authorised destruction authority (a “one-off” authorisation to destroy the specific records listed therein).

Detailed guidelines for the Disposal of Records are available at:


6.2 The Right to Information Act 2009 (TAS)

The *Freedom of Information Act* gives anyone the right to be provided with information in the University’s possession, unless the information is exempt under the Act. Freedom of information requests are processed by the Legal Office. For more information, see the Frequently Asked Questions about ‘Requests for Information’ on the Legal Office website, or contact the Legal Office directly.

6.3 The Personal Information Protection Act 2004 (TAS)

The *Personal Information Protection Act* regulates the University’s collection, maintenance, use and disclosure of personal information relating to individuals. The principles of the Act are reflected in the University’s Privacy Policy. All staff must comply with the Act and the Policy when collecting, holding, using or disclosing an individual’s personal information. ‘Personal information’ is any information or opinion (in any recorded format) about an individual whose identity is apparent or is reasonably ascertainable from the information or opinion. Below is a brief explanation of how the Act impacts upon record security procedures, however, for more detailed information about compliance, see the University’s Privacy Policy, or contact the Legal Office directly for advice.

The Act places obligations on the University to maintain the quality and security of the personal information it holds. Specifically, it must take reasonable steps to ensure that the personal information is accurate, complete, up-to-date and relevant to its functions or activities. It also must take reasonable steps to protect the personal information from misuse, loss, unauthorised access, modification or disclosure, and to destroy or permanently de-identify (subject to archival requirements) any personal information that is no longer needed for any purpose.

The Act also places restrictions on the use and disclosure that the University is able to make of the personal information it holds (except in limited circumstances, it can only be used or disclosed for the purpose for which it was collected). These
restrictions therefore help determine on the security and access measures that need to be adopted for information that is personal information.

7 Glossary

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Record</td>
<td>A record created, communicated and/or maintained by means of electronic equipment. Although this term can refer to analogue materials (e.g. videotapes), it generally refers to records held in digital form on magnetic or optical computer storage media</td>
</tr>
<tr>
<td>Folders</td>
<td>An aggregation of records allocated to a records category within the records classification scheme. A folder is constituted of metadata that may be inherited from the parent (records category) and passed on to a child (record).</td>
</tr>
<tr>
<td>Information</td>
<td>Any type of knowledge that can be exchanged. In an exchange, it is represented by data. An example is a string of bits (the data) accompanied by a description of how to interpret a string of bits as numbers representing temperature observations measured in degrees Celsius (the representation information).</td>
</tr>
<tr>
<td>Organisational Unit</td>
<td>College, Faculty, School, Centre, University Institute, other University Entity, Division, Section or University Business Enterprise.</td>
</tr>
<tr>
<td>Permanent Record</td>
<td>Permanent records are records that are deemed to have long-term value even after their immediate value as evidence of business activities has faded, usually for their potential historical/cultural value.</td>
</tr>
<tr>
<td>Record</td>
<td>Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. See University Records</td>
</tr>
<tr>
<td>Recordkeeping System</td>
<td>A framework to capture, maintain and provide access to evidence of transactions over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include: both records practitioners and records users a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices policy statements, procedures manuals, user guidelines and other documents that are used to authorise and promulgate the policies, procedures and practices the records themselves specialised information and records systems used to control the records software, hardware, other equipment and stationery.</td>
</tr>
<tr>
<td><strong>Records Management</strong></td>
<td>The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Retention period</strong></td>
<td>The length of time after the disposal trigger that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to disposal.</td>
</tr>
<tr>
<td><strong>Security Classification System</strong></td>
<td>A set of procedures for identifying and protecting official information whose disclosure could have adverse consequences for the University. The security classification system is implemented by assigning markings (such as 'unclassified' or 'confidential') that show the value of the information and indicate the minimum level of protection it must be afforded.</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>A set of processes to ensure that records are protected, accessible and managed in a cost-effective manner for as long as they are needed. This includes facilitating retrieval and use.</td>
</tr>
<tr>
<td></td>
<td><em>Adapted from: Standards Australia, AS-ISO 15489, Part 2, Clause 4.3.7.</em></td>
</tr>
<tr>
<td><strong>Temporary record</strong></td>
<td>A record that has value for a finite period of time only to the Australian community, the individuals and organisations that do business with the State and State Government agencies and statutory authorities themselves. Temporary records are needed by agencies to meet specific accountability requirements.</td>
</tr>
<tr>
<td><strong>TRIM</strong></td>
<td>HP TRIM is the University's Electronic Document and Records Management System (EDRMS). It manages electronic and hard copy records, enabling saving, editing, locating, tracking, archiving and disposal of information in the one system.</td>
</tr>
<tr>
<td><strong>University Employee</strong></td>
<td>Any individual employed by the University of Tasmania, including permanent, fixed-term and casual staff members and any contractors or consultants hired to perform work on behalf of the University.</td>
</tr>
<tr>
<td><strong>University records</strong></td>
<td>University records are records relating to the business activities of the University of Tasmania. The University owns all records created and received by individual employees as part of their day to day business, including research data, teaching materials and correspondence. Under the Archives Act 1983, the University’s records are State Records and must be managed and disposed of in accordance with the Act. See Records</td>
</tr>
</tbody>
</table>
### Vital records

The records without which an organisation could not continue to operate, i.e. those containing information needed to re-establish the organisation in the event of a disaster. Vital records are those that protect the assets and interests of the organisation as well as those of its clients and shareholders.

### 8 Versioning

<table>
<thead>
<tr>
<th>Former Version</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>Records Security Guidelines; Approved December 2006</td>
</tr>
<tr>
<td>Version 2</td>
<td>Records Security Guidelines; Reviewed August 2013 and Approved May, 2014. Amended in December 2016 to incorporate Colleges</td>
</tr>
</tbody>
</table>
Appendix 1 – University obligations under the Archives Act 1983 (TAS)

Detailed below is a brief summary of the important aspects of the Archives Act 1983 (Tas.) (“the Act”), as it relates to University operations generally and the obligations of University officers.

Section 3(1) of the Act defines a “record” as meaning: “…a document or an object that is, or has been, made or kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event, person, circumstance, or thing”.

Section 3(5) of the Act states that: “Without limiting the generality of the definition of the expression “record” in subsection (1) –

(a) the reference to a document in that definition includes a reference to any printed or written material; and
(b) the reference to a sound recording, coded storage device, magnetic tape or disc, microfilm, photograph, film, map, plan, or model or painting or other pictorial or graphic work”.

The above definition clearly encompasses computer and other electronic records stored on a coded device. The device could be hard or floppy disc.

Section 10 of the Act deals with the preservation and acquisition of State and other records. It states that records made for the purpose or in connection with the administration of a Government department or authority must be preserved until dealt with by the Act.

Section 11 of the Act deals with the transfer of State records to the Archives Office. This section states that when a record ceases to be used or referred to by an agency, or required to be made available for public use, that record must be transferred to the Archives Office. Records in existence for 25 years, unless exempted by writing, must be deposited in the Archives Office.

Section 15 of the Act deals with the ability of the University to restrict access to records which have been transferred to the Archives Office. It is implicit within the legislation that access to records will be unrestricted unless a restriction is specified at the time of transfer. The University may restrict access for given periods of time and/or restrict access to specific groups of users. Access to records may not be restricted for more than 75 years after the making of the record.

Section 20 of the Act deals with the disposal and destruction of records held by agencies. Section 20(1) states that persons must not destroy records in their possession. A person who contravenes this section is subject to financial penalty.

Section 20(5) of the Act states that a record used by means of any mechanical or electronic device or equipment, including a computer, if treated or modified in such a way that would prevent information being obtained, will be deemed to be destruction of the record.