



**UNIVERSITY OF TASMANIA
INFORMATION SECURITY FRAMEWORK**

**RECORD SECURITY
GUIDELINES**

This document is an initiative of the Records Management Unit.
Please visit our website at

http://www.utas.edu.au/governance_legal/rmu

UNIVERSITY OF TASMANIA INFORMATION SECURITY FRAMEWORK

RECORD SECURITY GUIDELINES

Purpose

These Record Security 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 Tasmanian ICT Security Framework, and the Records Management Policy and Records Management Guidelines, available on the Records Management Unit website http://www.utas.edu.au/governance_legal/rmu/policies.html

UNIVERSITY OF TASMANIAN INFORMATION SECURITY: RECORD SECURITY

Policy Statement

*“Staff of the University of Tasmania must ensure that records are created, captured, maintained, **secured** and disposed of in a way that complies with legal, administrative, cultural and business requirements”*

(from University of Tasmania Records Management Policy, Version 2, 2007).

Scope

This document applies to all records, whether paper-based or electronic, and includes information held in the TRIM corporate records management system. 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”.¹

Guidelines

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 consider:

¹ S3.15 AS ISO 15489.1 2002 *Records Management Part 1: General*.

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 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.

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 (eg business, political, or legislative) requirements beyond those provided by the recommended standard procedures; and
- 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:

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.

- 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 individual (eg HR personnel files);³
- Have specific legislative restrictions or requirements;⁴
- Cause serious financial damage to and/or lead to litigation against the University;⁵ and/or
- Cause serious loss of public confidence.

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, however, 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.

Recommended Standard Procedures

Paper Records	Electronic Records	TRIM Records
<ul style="list-style-type: none"> • Available to University employees who have a business requirement to access the records. • Available to authorised third parties. 	<p style="text-align: center;"><i>Access</i>⁶</p> <ul style="list-style-type: none"> • Available to workgroups, or clearly defined audience, enforced by user account belonging to a specified group. Groups can be based on organisation structure. • Available to authorised third parties. • Password policy implemented on systems. 	<ul style="list-style-type: none"> • Available to University officers having corresponding security level assigned to log-in: <ul style="list-style-type: none"> ○ <i>Public</i> – used for file &/or documents that are open to the public ○ <i>Unclassified</i> – used for files &/or documents having no restriction on access to University employees. ○ <i>Confidential</i> – limits access: files &/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).

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.

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.

⁶ Refer also to "Access to Archived Records held at the Archives Office of Tasmania Repository" – Records Management Guidelines, Version 2.0, "Retention, Disposal and Destruction of Records".

Recommended Standard Procedures

Paper Records	Electronic Records	TRIM Records
<i>Transmission</i>		
<ul style="list-style-type: none"> ➤ Must clearly show a return address in case of unsuccessful delivery. ➤ Must clearly identify the originating section/division. • No special designation when passed outside the organisation. • May be carried by internal courier service unsecured. • May be carried by ordinary postal services or commercial courier firms, provided the envelope/package is sealed. 	<ul style="list-style-type: none"> • Can be transmitted across external or public networks (including the Internet) without being encrypted. The level of information contained should be assessed before transmitting. • Accompanied by an outline of the legal responsibilities and disclaimer if received in error. 	<ul style="list-style-type: none"> • Can be transmitted across external or public networks (including the Internet) without being encrypted. The level of information contained should be assessed before transmitting. • Accompanied by an outline of the legal responsibilities and disclaimer if received in error.
<i>Storage ⁷</i>		
<ul style="list-style-type: none"> • Where possible, all records storage areas, such as the Records Management Unit, are to be secure areas with access provided only to authorised staff. • 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. 	<ul style="list-style-type: none"> • Computer systems controls – <ul style="list-style-type: none"> ○ Use of access controls and user accounts; ○ Use of appropriate controls and procedures governing applications management, maintenance, procurement, and development; ○ 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; ○ 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; ○ Systems, including University networks, should be monitored to detect deviation from the access control policy, and record monitorable evidence in case of security incidents. ○ Information, information processing facilities and network facilities should be protected from disclosure, modification, use or theft by unauthorised persons. Controls should be in place to minimise loss or damage. ○ 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 	<ul style="list-style-type: none"> • Official documents forming part of the University’s records must be captured into this corporate record-keeping system and/or retained within the business unit official record keeping systems.

⁷ 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, and in the *Guidelines for Storage of State Records in Non-Agency Facilities*, available on the Archives Office of Tasmania website <http://www.archives.tas.gov.au/govservice/policies.htm>

business continuity planning.

Recommended Standard Procedures

Paper Records	Electronic Records	TRIM Records
<ul style="list-style-type: none"> • Official files 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, to ensure appropriate record tracking can be undertaken and follow ups for return of files can be made. • Mobile worker should ensure that official information, particularly if it is sensitive, is appropriately protected. This may be achieved by: <ul style="list-style-type: none"> ○ Locking information away in an appropriate security container; ○ Locking of vehicles; ○ Locking the door to the office, study or work area; ○ Disposing of waste appropriately; ○ Ensuring documents cannot be overviewed (eg by telephotography); or ○ By a combination of these and other actions. 	<p style="text-align: center;"><i>Home Based or Mobile Workers</i></p> <ul style="list-style-type: none"> • 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. • Refer further to ITR Security framework. 	<ul style="list-style-type: none"> • Access via VPN • 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.
Destruction		
<ul style="list-style-type: none"> ➤ Secure destruction of the record after the time specified for retention, as determined by the State Archivist, has elapsed. ➤ For detailed guidelines relating to the disposal of records see http://www.archives.tas.gov.au/legislative/staterecords/guidelines_list/guideline_02 and the Records Management Guidelines, "Retention, Disposal and Destruction of Records" 		
<ul style="list-style-type: none"> • Depending on the degree of confidentiality and volume of material, three methods are available to University staff: <ul style="list-style-type: none"> ○ 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 ○ Ephemeral material may be recycled by pulping or normal waste disposal processes. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • TRIM has built in mechanisms regarding destruction of electronic records from the data base.

Alternate Procedures

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 table lists some procedures staff may wish to implement should a higher level of security be required. The table assumes the standard procedures above as a minimum.

Alternate Procedures

Paper Records	Electronic Records	TRIM Records
<i>Access</i>		
<ul style="list-style-type: none"> ➤ Limiting access to permanent records transferred to the Archives Office of Tasmania • Strict controls on which members of University staff are authorised to have access to the records. 	<ul style="list-style-type: none"> • Strict controls on membership of user groups. • Audit trail of all access to information. • Separate read and write access controls. • Storage of information in separate and identified volumes or directories. 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ Assigning the “<i>Confidential</i>” security level to the record – this limits access to the file and/or document by making them accessible only to authorised officers having the corresponding log-in. ○ Assigning “<i>Caveats</i>” 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 “<i>Access Control</i>” mechanism. This provides additional ad hoc or group security at document 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 &/or requirements of matter to which document relates. ○ Full audit trail of access to information.
<i>Transmission</i>		
<ul style="list-style-type: none"> ➤ Accompanied by an outline of the legal responsibilities and disclaimer if received in error. ➤ Information must be clearly marked to indicate alternate procedures are required. ➤ Security markings must not be visible in message header or external envelope. • Use of sealed envelopes when carried by internal courier. • Where risk is very high, use of double envelopes when posted or carried by commercial courier firms. 	<ul style="list-style-type: none"> • Use of encryption when transmitted across external or public networks (including the Internet). • Where the risk is extreme, use of encryption when transmitted between University sites. • Refer further to ICT Security Framework. 	<ul style="list-style-type: none"> • Use of encryption when transmitted across external or public networks (including the Internet). • Where the risk is extreme, use of encryption when transmitted between University sites. • Refer further to ICT Security Framework.
<i>Storage</i>		
<ul style="list-style-type: none"> ➤ Where the risk is very high, use of security guard or officer. ➤ Where the risk is very high, use of security Committee assigned to manage restricted information. ➤ Provision of sealed off, fire resistant area of building for storage of computer systems and/or physical records. • Stored separately to other information. • Stored in lockable cabinets or open shelving or a controlled area with security perimeter and restricted access. 	<ul style="list-style-type: none"> • Encryption when stored in a device or location that is not physically secured. • Refer further to ICT Security Framework. 	<ul style="list-style-type: none"> • Encryption when stored in a device or location that is not physically secured. • Refer further to ICT Security Framework.
<i>Home Based or Mobile Workers</i>		
<ul style="list-style-type: none"> • Records being transported are secured in locked containers. • Mobile worker/home-based worker must ensure that sensitive official information is appropriately protected, by: 	<ul style="list-style-type: none"> • Mobile worker/home-based worker to ensure that official information, particularly if it is sensitive, is appropriately protected. This may be achieved by logging of the computer at the conclusion of the work period. 	<ul style="list-style-type: none"> • 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 of the computer

- Locking information away in an appropriate security container;
 - Locking of vehicles;
 - 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.
- Where the risk is very high, use of encryption.
- at the conclusion of the work period.
 - Where the risk is very high, use of encryption.
-

Alternate Procedures

Paper Records	Electronic Records	TRIM Records
Destruction		
<ul style="list-style-type: none"> ➤ For detailed guidelines relating to the disposal of records see http://www.archives.tas.gov.au/legislative/staterecords/guidelines_list/guideline_02 and the Records Management Guidelines, “Retention, Disposal and Destruction of Records” • Secure destruction by shredding of the record after the time specified for retention, as determined by the State Archivist, has elapsed. • Disposal of paper records via security shredding service. 	<ul style="list-style-type: none"> • Measures which may be taken depend upon the media: <ul style="list-style-type: none"> ○ <i>CDs, microfilm, microfiche</i> – depending upon risk, select one or a combination of: (i) physical destruction (shredding); and/or incineration. ○ <i>Laser printer & copier drums</i> – 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. ○ <i>Magnetic media</i> – depending on risk, select one, or a combination of: (i) sanitised by low-level reformatting or similar activity; (ii) de-magnetised and so rendered useless; and/or (iii) physical destruction. ○ <i>PDA's, flash ROM & other emerging removable media</i> – depending upon risk, select one, or a combination of: (i) sanitised by low-level reformatting or similar activity; and/or physical destruction. • Refer further to ICT Security Framework. 	<ul style="list-style-type: none"> • TRIM has built in mechanisms regarding destruction of electronic records from the data base.

Application

Staff are to apply the model to records held by the University. In practicable terms, this requires that the employee who creates or receives the record is to apply the appropriate record security procedures.

Legislative Framework

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:

www.archives.tas.gov.au/govservice/policies.htm

The Freedom of Information Act 1991 (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.

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, the Frequently Asked Questions about ‘Privacy’ on the Legal Office’s website, 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.

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.