1. PURPOSE

As a public agency, the University is required to comply with a range of government policies, standards and procedures. Key external recordkeeping policies and standards are provided by the Public Record Office Victoria. It is a requirement of Strategic Management Standard PROS 19/03 that a records management strategy be regularly developed, resourced, and systematically implemented with progress being monitored and reported on1.

The purpose of this document is to outline:

- what Records plans to achieve in 2022;
- how Records supports and aligns to the broader SSE and eSolutions goals which aim to enable and support Impact 2030;
- the risk management approach for lowering the impact and likelihood of a data breach, exacerbated by the over retention of data. There are many types of recordkeeping risk events, however the over retention of data is a known risk event that has been identified across structured and unstructured University IT environments and is therefore the focus of this year’s Strategy;
- how Records will monitor and report on progress made against this strategy.

2. BACKGROUND

The evolution of Records within eSolutions:

3. KEY GOALS

Streamline and Simplify recordkeeping concepts so they are fit for purpose

**IF YOU:** can explain key recordkeeping concepts without the jargon  
**THEN YOU:** help colleagues to understand why recordkeeping should matter to them  
**THEN YOU:** create opportunities for a shared understanding of recordkeeping to occur  
**THEN YOU:** can leverage that shared understanding to improve recordkeeping practices

Utilise partnerships to improve visibility over the University’s recordkeeping landscape

**IF YOU:** know where the records are located  
**THEN YOU:** can check how well they are/aren’t being managed  
**THEN YOU:** identify recordkeeping risk events  
**THEN YOU:** reduce the likelihood/impact of records being over retained *

Identify key recordkeeping risk events in order to provide targeted recordkeeping advice to the business

**IF YOU:** have established partnerships with colleagues around a shared understanding of recordkeeping  
**THEN YOU:** work with those colleagues to identify and address recordkeeping risk events (e.g. over retention)  
**THEN YOU:** are reducing the likelihood and impact of an adverse recordkeeping event  
**THEN YOU:** increase the recordkeeping maturity of the business

See Appendix 1 for a breakdown of the associated tasks aligned to each goal.
4. WHY DOES RECORDKEEPING MATURITY MATTER?

Records sits within SSE (Support Services and Engagement). As of December 2021, the SSE 2022 goals and its relationship to Impact 2030 are as follows:

The Records goals for 2022 supports the wider SSE goals by:

- making recordkeeping advice more accessible and easier to apply;
- to enable, empower and engage our customers by simplifying recordkeeping practices so they can be implemented as required;
- to drive down the likelihood and impact of adverse recordkeeping risk events occurring (e.g.: over retention of data);
- to ensure existing services dependent on accurate recordkeeping maintain their value;
- to enable Impact 2030.

5. RISK MANAGEMENT & RECORDKEEPING

5.1 University Context

The University’s Risk Management Statement (approved by Council. Meeting 4/2019) notes under ‘Information and Communication Technology’ that:

The integrity of our information and the robustness of our systems enables our research and teaching, and protects our reputation. In an increasingly threatening cyber environment, we have the lowest tolerance for risks where our systems and our information will be compromised by either external threats or internal misuse. Controls must be in place to ensure:

- Our staff, students and partners trust us to protect the information they provide to us.
- Specialist systems including that of our outsourced providers are secure and well managed.²

University records are contained within the information that the University owns and seeks to protect from external threats and internal misuse. Within the University’s Risk Management Framework, the Records program is considered a ‘non-core (support) operation that directly relates to the University’s operations.”³

³ Monash University Risk and Compliance Manual, V. 3 (p.7)
Records is currently focused on reducing the likelihood and impact of Key University Risk 12: Monash University experiences a significant cyber breach/attack by targeting risk events at an operational level that are likely to exacerbate a cyber breach/attack through the over retention of data.

The risk matrix and risk response treatment guidance used in this assessment have been adapted from that used by the University Risk and Compliance Office.

The risk response definitions for this assessment are:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>The risk can be accepted. eSolutions can adopt this model. Monitoring of the model implementation is required. Additional risk mitigation is recommended but not essential.</td>
</tr>
<tr>
<td>Medium</td>
<td>The risk can be accepted provided reasonable controls are in place. eSolutions can adopt this model ensuring the appropriate management and risk controls are implemented.</td>
</tr>
<tr>
<td>High</td>
<td>The risk can be accepted provided strict monitoring is in place. eSolutions can adopt this model with caution. Close management of the model will be required to ensure risk exposure is kept to a minimum.</td>
</tr>
<tr>
<td>Extreme</td>
<td>eSolutions are strongly recommended to avoid this model, to adopt it would expose the University and eSolutions to unacceptable levels of risk.</td>
</tr>
</tbody>
</table>

5.2 Risk Identification

<table>
<thead>
<tr>
<th>Risk Event (Title)</th>
<th>Who would be most impacted?</th>
<th>Likelihood</th>
<th>Consequences/Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>A data breach occurs across various University enterprise systems, exposing sensitive/highly sensitive data that is past its due date for destruction.</td>
<td>Current and ex University staff and students.</td>
<td>MEDIUM</td>
<td>Breach of Privacy and Data Protection Act 2014 (Vic), the Health Records Act 2001 (Vic), as well as the European Union General Data Protection Regulation 2016/679 (EU) could include fines depending on the nature and extent of the breach. If there is a requirement to notify affected individuals of the breach, this could take up considerable time and financial resources. Reputational damage and loss of public trust (e.g. ANU data breach - <a href="https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach">https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach</a>)</td>
</tr>
</tbody>
</table>

5.3 Risk Analysis

If a data breach occurred across various University enterprise systems, exposing sensitive/highly sensitive data the consequences would vary depending on the nature and extent of the breach and the type of data involved. Any breach would be exacerbated if the data exposed contained sensitive or highly sensitive data that the University had kept longer than it was permitted to under the University’s Retention and Disposal Authority.

Understanding the true extent of how much data is currently being over retained across the University is difficult to ascertain. As this data is likely to be present across structured environments such as enterprise systems, as well as unstructured environments like S: Drive, Google, Gmail etc.

Up until the last 12 months, the existing controls from Records have been passive and relied mostly on the presence of the University Retention and Disposal Authority (RDA) being available on the Archives & Records website. When customers or colleagues have sought out data retention information, we have provided the advice and then left them to it. The theory being that Records only has to provide the advice and the likelihood and significance of a risk event occurring will be significantly reduced While some University staff may be aware of the RDA and how to action it, there are many reasons why just providing disposal advice and not conducting any ongoing follow up has limited impact in treating this type of risk event.

---

5.4 Risk Evaluation
As the University overall, has a low risk appetite for any ethical or regulatory breaches the risk options to address this include:

- reducing the level of risk where a risk event related to the over retention of data has been identified as well as
- sharing the risk with the relevant parties.

In most instances, Records does not have custody or control over the records involved in these kinds of risk events. Records requires the parties who manage the data to take the necessary steps (under Records advice), such as identifying and destroying data that is due for legal destruction in accordance with the RDA. Records needs to then actively monitor these risks with the relevant parties co-operation, report on the outcomes and escalate concerns to management when necessary. A key part of this evaluation requires the Records team to be able to understand and communicate the recordkeeping risk events within the context of the IT systems that are being used.

5.5 Risk Treatment
Going forward Records will continue be taking a more active role in identifying and communicating recordkeeping risk events in partnership with the data owners through projects such as:

- S: Drive Project (in partnership with TS)
- Recordkeeping Assessments

Records must engage with colleagues and customers in more innovative ways by providing specific recordkeeping advice that is accessible and specific to the risk event that needs managing. Records staff involved in work such as the S: Drive Project and Recordkeeping Assessments need relevant IT skills and knowledge to be able to communicate general retention and disposal advice to technical teams in a meaningful way. They then need to be able to work with technical support teams to devise solutions to enable specific retention and disposal advice to be implemented in both structured and unstructured IT environments. A more active role also involves being committed to following up with the technical teams, service and product owners after the initial consultation through regular monitoring and review activities as outlined below.

6. MONITORING AND REPORTING

6.1 Monitoring Activities to be undertaken in consultation with colleagues and customers

Recordkeeping Assessments (RKA) contain an ‘in-built’ follow up clause if the initial system assessment does not meet the recordkeeping requirements. This provides the customer with the opportunity to resubmit the assessment for re-evaluation. Records staff then indicate to the customer that a follow up will occur to ensure the agreed to actions have been implemented.

Ongoing Quality Reviews are conducted in TRIM by Records to assess how the customers are managing their records in TRIM. A written Quality Review will make suggestions for improvement, offer additional training or advice where required and set timelines for follow up.

Recordkeeping Audits are a tool that can be exercised when a known recordkeeping risk event exists and no prior interventions have resulted in lowering the likelihood or consequence of the risk occurring. This type of monitoring would only be instigated under the direction of eSolutions Senior Executive.

---

7 The S: Drive Project commenced in the second half of 2021. The purpose of the project is to assist Technology Services (TS) in gaining better visibility across the S: Drive landscape. The outcome is to provide additional security to folders held on the S: Drive which contain sensitive/highly sensitive data. Records role has been to help design the survey used to gain visibility of what is held on the S: Drive as well as conduct interviews with customers to assist them to fill the survey in. The survey information is then handed back to TS to action. Records is able to build relationships with the customers through this work and where appropriate has been able to provide recordkeeping advice as well.
8 A Recordkeeping Assessment (or RKA) is used as a first step to assess whether a system (either existing or one that is ready to be released) meets some basic recordkeeping requirements. They are mostly submitted by Service Delivery Managers across eSolutions who are working on new product releases. However, the form can be used by any staff member who wants to get a better understanding of whether any new or existing system meets basic recordkeeping requirements as outlined in the Public Record Office of Victoria Standards.
6.1 Key Reporting

The two main forms of reporting for Records include:

- **Weekly reports on RM TRIM & BAU activity.** These reports detail the number of documents registered in TRIM during the past week, which are then compared against figures from the previous year. These reports also provide an analysis of the data as well as an update on any BAU activities that have taken place during the previous week. These reports are sent via email to the Manager, BCM, Archives and Records.

- A Quarterly Maturity Model Report (compiled with Archives) tracks the recordkeeping maturity levels of recordkeeping and records held within the custody of the two programs, as well as tracking the state of recordkeeping across the rest of the University. This report includes details around progress and follow up results from activities such as Recordkeeping Assessments and the S: Drive Project.
APPENDIX 1 – TASKS 2022

KEY TASKS

The following tasks support the strategic goals of Records in 2022.

<table>
<thead>
<tr>
<th>GOAL: Streamline and simplify recordkeeping concepts so they are fit for purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Continue to roll out the S: Drive project across University business units and faculties</td>
</tr>
<tr>
<td>• Undertake RKA work on demand as well as identify opportunities to conduct RKA work where a possible risk event has been identified through the S: Drive project.</td>
</tr>
<tr>
<td>• Update and transform the Records website to reflect changes that have taken place within Records.</td>
</tr>
<tr>
<td>• Continue to seek out and implement integration opportunities with areas who are eligible to add and/or bulk action their records into TRIM.</td>
</tr>
<tr>
<td>• Explore ways to bulk action records in shared drives (in conjunction with TS, as part of the next stage of the S: Drive work).</td>
</tr>
<tr>
<td>• Continue to develop the recordkeeping literacy program via more “Recordkeeping Stories Podcasts”.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOAL: Utilise partnerships to improve visibility over the University’s recordkeeping landscape</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create Road Map for the S: Drive Project (in consultation with TS) in order prioritise the next stages of the project. This involves TS providing RM with ‘larger chunks’ of the S: Drive path names in order for RM to assess which business units and faculties can be approached next for the completion of surveys/interviews.</td>
</tr>
<tr>
<td>• Complete S: Drive Project survey/interview work of the areas identified as priority areas via the aforementioned Road Map.</td>
</tr>
<tr>
<td>• Identify and engage with other partners within the business (e.g. re-establish relationship with Cybersecurity) and look for additional collaboration opportunities to address University recordkeeping challenges.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOAL: Identify key recordkeeping risk events in order to provide targeted recordkeeping advice to the business</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Undertake Recordkeeping Assessments (RKA’s) and all necessary follow up work:</td>
</tr>
<tr>
<td>o when eSols colleagues request the service</td>
</tr>
<tr>
<td>o as identified through related project work (e.g S: Drive Project)</td>
</tr>
<tr>
<td>• Undertake recordkeeping review of at least one business unit who currently uses TRIM and undertake all necessary follow up work:</td>
</tr>
<tr>
<td>o e.g. Buildings &amp; Property Division</td>
</tr>
</tbody>
</table>
BAU TASKS

These tasks indirectly support the “Key Tasks” outlined above. For example, the maintenance of TRIM (University’s enterprise recordkeeping system) is required as it contains over 2,751,900 University records. Much of the University is moving towards managing records ‘in-place’ across the 800 + systems currently supported by eSolutions. There is however, an ongoing requirement for TRIM for both creating and accessing records especially with customers such as HR, Disability Support Services, some areas of student administration, OGC and others.

GOAL: TRIM maintains its status as a secure, efficient, fully supported enterprise recordkeeping system

- Ensure DR Test Plan for TRIM is implemented for 2022 and a DR Test is scheduled and completed successfully, with learning outcomes incorporated into the test plan for the next DR Test. This is work being undertaken by TRIM’s internal support team (Shared and Campus Services – Application Administration).
- Support TRIM’s Technical Support Agreement Contract renewal process for April 2022.
- Co ordinate TRIM Upgrade (version to be determined in conjunction with vendor closer to the time) by mid-2022.
- Maintain currency of TRIM security groups, user groups, etc as required as part of standard maintenance process.

GOAL: Annual destruction of both hard copy and electronic files held under the custody of Archives and Records occurs in a timely manner

- Ensure all hard copy file destruction for student files (that was scheduled for 2021 but delayed due to COVID-19 restrictions) is undertaken in 2022, when safe to do so.
- Ensure all relevant student files held in TRIM are closed, sentenced, made inactive and actioned in accordance with relevant RDA sentencing requirements.
- Identify which files (outside Student Files and those managed by HR) maintained in TRIM require action in terms of sentencing, closure, disposal etc. Update existing Annual Destruction Road Map document for this exercise and execute the Road Map accordingly.

GOAL: Maintain existing Helpdesk support and training services for TRIM as required

- Continue to manage tickets registered in MyServices in a timely manner so that they meet SLA targets and do not fall into the breached category.
- Review content in the Online TRIM Training modules held in MyDevelopment – to ensure it is kept up to date.
- Review existing SOPS and ensure they are up to date and easy to locate.