Records and Information Risk Assessment Guide

1. Purpose

The purpose of this guide is to assist System and Information Owners to determine the level of risk associated with the University records (physical and digital) they are responsible for, and to apply a risk-based approach to the management and storage of records. High risk and/or high value records require more rigorous management processes, whereas the low risk and/or low value records have more flexibility in their record management provided that key recordkeeping and privacy obligations are met.

2. Scope

This guide applies to University records that are subject to and defined by the Records and Information Management Policy.

This guide should be read in conjunction with the Information Security Data Classification and Handling Manual which outlines how the sensitivity of records and information is used to determine the controls required to protect them.

3. Definition

a. **"high risk records"** means those University records that are created in high risk business processes or functions, or received in high risk areas of the University, and are considered at a level of risk that is outside the University's risk appetite should they be misused, released inappropriately, inappropriately accessed and altered, lost, damaged or destroyed prematurely. They are required to conduct core functions, to make key decisions and to give evidence of those key decisions at a later date: high risk records demonstrate the performance of legislated functions, the interactions with and entitlements of students, clients and employees. High risk records may also relate to the requirement for additional security, for example to protect records containing sensitive, classified, or personal information.

b. **"high value records**" means those University records, information and data that enable the University to continue their functions, provide a service and respond to Royal commissions, inquiries, audits, investigations and legal issues. They have continuing business value to the University and/or archival value to the State of New South Wales.

Examples of records that are considered to be high risk and/or high value are records that document;

- individual's rights, entitlements, wellbeing, responsibilities. For example, qualifications issued by the University, student records, clinical or client records, HR records, misconduct and disciplinary records, creditor records, student and staff related policies, Rules and by-laws,
- university's rights, entitlements, responsibilities. For example, government directives or approvals, strategic contracts, the University's copyright and IP, high level committee records including Council and Academic Senate and research grant applications/revenue,
- plans, academic transcripts, final approved curricula and register of graduates,

- final datasets/papers collected during research projects
- significant investment. For example, records of projects relating to buildings and infrastructure,
- activities that could be open to potential fraud or corrupt behaviour, or allegations of such, if not properly controlled. For example, allocation of student results, student or staff entitlements, expenditure of money. Note that good recordkeeping processes in such activities supports accountability, either disproving allegations or assisting to identify or monitor potential fraud, and
- records identified as "State archives". For example, qualifications, high level committee minutes, establishment records such as records pertaining to the establishment of new organisational structures, significant research data, annual reports, strategic records of decisions and related due diligence related to University activities that are identified as being a high or critical risk in accordance with the Business Continuity Management Framework.

4. Risk Impacts

There are three key elements that affect the level of risk associated with records management practices:

- **Business needs** - The purpose of the record and the potential impact on the University's business if the record is lost, inaccessible, incomplete, or subject to unauthorised access, modification or disclosure.
- **Retention periods** - How long the record needs to be kept. Legislated retention requirements are often designed around risk. The longer the retention period, the more important the record may be, both for the business and for the wider community.
- **Legislative requirements** - Records that are required to meet legal obligations such as Government Information Public Access (GIPA), subpoenas, search warrants, and mandatory government reporting requirements.

4.1 Additional risk considerations also include:

- Where records are held: for example, whether your records are stored in a shared office space, off-site in a dedicated storage facility, on a staff members laptop, in a suitably architected (software) environment or supported University environment.
- Privacy and sensitivity considerations: for example, if the records contain personal (sensitive and health) information, Tax File Numbers (TFN), banking details. Retaining these records beyond the minimum legal retention requirement can increase privacy risks.

4.2 Issues that may increase the level of risk include:

- inadequate recordkeeping functionality in information systems;
- inadequate contractual controls to manage and protect records held in hosted environments;
- technological obsolescence;
- building works, both minor and major, impacting on storage locations;

- external disasters (e.g., flood, earthquake, terrorism, cyber-crime, fire);
- internal disasters (e.g., broken pipes, fire);
- fraudulent activities and human error, including lack of appropriate staff education and training in recordkeeping requirements;
- lack of or ineffective policy and procedures; or
- use of inadequate storage areas (e.g., poor security or environmental conditions).

The likelihood that records may be lost or inaccessible increases as the retention period increases. For example, records may be affected by:

- technological failure or obsolescence of hardware and/or software;
- corruption of digital documents;
- changes in security standards, legislation, community expectations;
- arrangements with Software as a Service (SaaS)/vendor hosted systems, including any change in vendor, contractual obligations, or where a contracted service may cease; or
- lost/misplaced records located in forgotten storage locations.

An example of risk mitigation would be to store records and information that have longer retention requirements in the University Records Management System (TRIM), or to store physical records in an approved University storage location in consultation with Records Governance Services.

5. How to apply risk levels to records

The below steps and tools will assist you in applying risk levels to your records.

Note: The Records Inventory template is provided to assist with identifying the records that your Organisational Unit keeps/manages, and recording important information about them. Selecting an individual heading will display additional information to assist you in populating the required Inventory information correctly.

1. In your Records Inventory, list all record types (Column A) that your Organisational Unit keeps/manages. Refer to Table 2 (Appendix 1) for examples of types of records.

Note: A record is any document or other source of information which documents any of the following in the course of carrying out a University function or activity:

i. a decision (in the positive or negative),
ii. a binding commitment,
iii. research,
iv. deliberation, advice, evidence, or actions.

Records may be in any physical or digital format (including but not limited to paper based records; databases; emails; scanned documents; records created in collaboration sites such as (but not limited to) MS365 – Teams, SharePoint, OneDrive; records created in cloud based third party applications; microfilm; tape; photos; video footage; webpages; social media content; maps and research data.

2. In your Records Inventory, for every record type add:

- a description (Column B),
- whether it is the source of truth for the University (Column C),
- the record format (Column D),
- the current storage location (Column I).

3. For every record type listed in your Records Inventory, use the Risk rating table (Table 1), to determine the severity of the risk associated with the records and information e.g., if the record and information were lost or stolen what would the severity rating be;

a) Insignificant
b) Minor
c) Moderate
d) Major or
e) Severe

Use the examples provided in the Risk rating table to assist in determining the severity of the risk. Where a record type has multiple associated risks, use the highest severity. E.g. if Operational Risk is Moderate, and Reputation Risk is Major, use Major as the severity of the risk.

In the Records Inventory populate Column G with the identified severity of risk using the drop-down option for each record type.

4. For every record type listed in your Records Inventory, **identify the retention requirements utilising the** *Disposal Authorities* **that are located on the University's Records Governance web page, or the examples provided** in Table 2 (Appendix 1).

In the Records Inventory populate Column E with the identified Retention Schedule and Column F with the applicable retention requirement for each record type.

Note: Records Governance Services can assist with the identification of retention requirements. If the organisational unit populates this information themselves, Records Governance Services will still check that the information entered is accurate and liaise with the organisational unit where necessary to discuss, and correct if required.

5. Once you have identified the retention requirements (Column F) and the severity risk rating (Column G), use the **Record Risk Matrix** below to identify the level of risk (Risk Level) that applies to each record type in your Records Inventory. Then, add this to Column H in the Records Inventory for each record type.

6. With reference to **5.1 Record controls**, work with Records Governance Services to discuss and determine an agreed upon storage location for each record type in your Records Inventory. Then, where applicable, implement any further record controls recommended by Records Governance Services to manage the risks.

Table 1 – Risk rating table

Use this table to determine the severity of risk to records and information:

	Severity				
	Lowest ⟷				Highest
Impact / Consequence	Insignificant	Minor	Moderate	Major	Severe
Examples of consequences if information became inaccessible, incomplete, or subject to unauthorised access, disclosure or modification					
Operational Risk **For example,** loss/inaccessible research data stored on an unsupported hard drive resulting in an inability to meet contracted reporting obligations for research grants, or the loss of evidence relating to IP.	❖ Some localised inconvenience, but no impact to the University.	❖ Disruption to operations with no permanent or significant effect on the University.	❖ Some impact on the University's operational performance. ❖ Less impact on strategic goals in the medium term.	❖ Significant effect on operational performance.	❖ Achievement of operational and strategic goals in the medium term jeopardised. ❖ Ability of the University to continue to function under threat.
Regulatory Risk **For example,** the inability to meet external audit, GIPA or subpoena obligations because of records being deleted prior to meeting legal retention requirements.	❖ Breach of legislation, contract, rule or policy that have no impact on the relationship with the third party or legislator. ❖ No litigation or prosecution and/or penalty.	❖ Regulatory consequence limited to standard inquiries and some minor corrective action in the short or medium term ❖ Breach of legislation, contract, rule or policy that may have an impact on the relationship with the third party or the legislator, but no long-lasting effect.	❖ Breach of legislation, contract, rule, or policy leading to escalated legal enquiries. ❖ Regulatory or legal consequence limited to additional questioning or review by legislator.	❖ Breach of legislation, contract, rule, or policy leading to possible legal action. ❖ Possible litigation or criminal prosecution and/or penalty. ❖ External enquiry or regulatory review and/or possible negative sanction by a regulatory body.	❖ Breach of legislation, contract, rule, or policy leading to significant and costly legal action with widespread potential impact for the University. ❖ Litigation or criminal prosecution and/or substantial major negative sanction by a regulatory body.
Health and Safety Risk **For example,** where the loss or inaccessibility of asbestos records results in a failure to implement asbestos risk controls leading to asbestos related health issues on staff, students and visitors	❖ No impact to employees / WHS.	❖ First aid or medical treatment required but no lost time	❖ Continuity of employment concerns across the University. ❖ WHS incident requiring significant medical attention. ❖ WHS event reported and investigated.	❖ Significant (up to 15%) loss of staff contained to one college / division. ❖ Widespread damage to staff morale. ❖ WHS event causing severe injury, or negative environmental impact and external authorities notified.	❖ Significant loss of staff extending to the entire University (over 15%). ❖ WHS event causing serious permanent injury, death or environmental impact, leading to costly action and widespread impact on the University and/o senior staff.

Records and Information Risk Assessment Guide

	Severity				
	Lowest ⟷				Highest
Impact / Consequence	Insignificant	Minor	Moderate	Major	Severe
Financial Risk **For example,** the loss of financial records results in re-work or inability to produce an audit trail.	❖ Less than 1% of budget or up to $25K.	❖ 1 to 2% of budget or $25-50k.	❖ 2-5% budget or $250k – 1m.	❖ 5-10% budget or $1-5m.	❖ Over 10% of budget or over $5m.
Reputation Risk **For example,** unauthorised disclosure of information to third parties resulting in public scrutiny, litigation, or reduced engagement with students or funding bodies.	❖ No impact to reputation. ❖ Minimal or no stakeholder interest.	❖ Issue raised by students and/or local press for a limited time. ❖ Minimal local public or media attention (including social media) and complaints. ❖ Short term minor political attention. ❖ Minimal damage to reputation.	❖ Student and/or community concern. ❖ National media coverage and external criticism. Reputation impacted with some stakeholders.	❖ Loss of student confidence in a School or College. ❖ Sustained adverse national media and public coverage. ❖ Reputation impacted with a significant number of stakeholders. Breakdown in strategic and or business partnership.	❖ Loss of student confidence in the University. ❖ Reputation and standing of the University affected nationally and internationally. ❖ Reputation impacted with majority of key stakeholders. ❖ Significant breakdown in strategic and or business partnerships.
Service Levels **For example**, the loss of contract agreements relating to buildings, infrastructure, strategy.	❖ Loss of less than one day of teaching, research and/or business functions.	❖ Loss of one full day of teaching, research and/or business functions.	❖ Loss of 2-7 days of teaching, research and/or business functions.	❖ Loss of two weeks to two months of teaching, research and/or business functions.	❖ Loss of over two months of teaching, research and/or business functions.
Example information types	❖ College and staff directory information. ❖ Published research data.	❖ Course descriptions. ❖ Course catalogues.	❖ Business unit process and procedure. ❖ Unpublished intellectual property. Departmental intranet.	❖ Student and Staff HR Data. ❖ Organisational financial data. ❖ Current exam material. ❖ Research Data (containing personal data).	❖ Data subject to regulatory control. ❖ Employee relations and complaints information ❖ Medical, Children, Young person's and credit card information. ❖ Research data (containing personal medical data).

Record Risk Matrix

Business impact/consequences of records being lost, inaccessible, incomplete, or subject to unauthorised access, disclosure, or modification

How long you need to keep records based on the Disposal Authorities

Business Impact / Consequences	Insignificant	Minor	Moderate	Major	Severe
40 years +	High	High	High	Extreme	Extreme
21-39 years	Medium	Medium	High	Extreme	Extreme
11-20 years	Low	Medium	Medium	High	Extreme
6-10 years	Low	Low	Medium	Medium	High
1-5 years	Minimal	Low	Low	Medium	Medium

5.1 Record controls:

The University Records Management System (TRIM) is a purpose-built records management system with built in retention and disposal authorities. Storing and managing records within TRIM is the best way to deliver compliance with policy and State regulations, ensure records are not over or under retained, and ensure our records are authentic, reliable, accessible, useable and secure against unauthorised alteration and destruction.

A University Approved Information System is an information system supported by the University which has been assessed and endorsed by both Records Governance Services as having suitable recordkeeping functionality (either natively, or by taking action to address recordkeeping gaps); and Digital Technology Solutions for acceptable security functionality.

Ideally, all University records should be stored within TRIM or a University Approved Information System, however this is not easily achievable due to the amount of business now conducted within the Office365 environment.

Therefore, below are three options for storing and managing University records based on the risk level associated with the records. Records Governance Services provides the below options to strike a balance between protecting the University and allowing our staff to conduct their business as efficiently as possible.

a) For records with a **minimal or low** risk level there may be flexibility in how records are managed providing key recordkeeping obligations are still met, including timely and authorised destruction, security, and privacy consideration (protecting personal, health and sensitive information). **These records could be retained and managed in-place** rather than moving these to the University Records Management System (TRIM). If these records are within an information system (this includes Office365 applications), then it should be a University Approved Information System (see below **Note** which lists the requirements for a University Approved Information System).

b) For records with a **medium** risk level, Records Governance Services recommends that these be captured formally into the University Records Management System (TRIM). However, there may be flexibility in how records are managed providing that reasonable records management practices are in place and key recordkeeping obligations are still met, including protecting records with long retention requirements, timely and authorised destruction, security, and privacy consideration (protecting personal, health and sensitive information). **These records could be retained and managed in-place** rather than moving these to the University Records Management System (TRIM). If these records are within an information system (this includes Office365 applications), then it should be a University Approved Information System (see below **Note** which lists the requirements for a University Approved Information System).

c) For records with a **high or extreme** risk level more rigorous recordkeeping processes will need to be applied. Where you have identified that your records have a high or extreme risk level, consult with Records Governance Services to determine the required risk treatment measures and to ensure rigorous recordkeeping processes are put in place. This will be particularly relevant when assessing recordkeeping in information systems, especially those that are hosted in SaaS environments. **These records must be retained and managed in the University Records Management System (TRIM) or a University Approved Information System** (see below **Note** which lists the requirements for a University Approved Information System).

Note: For an information system to be endorsed as a University Approved Information System it must meet the below requirements:

- it must be a system supported by the University, and
- it will need to be assessed and endorsed by Records Governance Services as having suitable recordkeeping functionality (either natively, or by taking action to address recordkeeping gaps), refer Business Systems Assessment Checklist for Recordkeeping, and
- it will need to be assessed and endorsed by Digital Technology Solutions for acceptable security functionality.

Refer to the Information Security Data Classification and Data Handling Manual for further controls to mitigate risk.

Appendix 1

Table 2 – Examples of minimum legal retention requirements for university records

Type of records	Retention Schedule	Retention Requirements
Teaching		
Student administration records	GA47-1.1.1	Retain minimum of 7 years after completion or discontinuation of course or program of study by student
Professional placement reports	GA47-2.1.3	Retain minimum of 50 years after completion of course of study
Final results obtained by student	GA47-1.2.4	Retain minimum of 75 years after action completed
Final approved curricula	GA47-2.4.1	Required as State archives
Masters of examination papers	GA47-2.3.2	Retain minimum of 15 years after superseded
Register of graduates/records confirming award/receipt of a qualification	GA47-1.2.3	Required as State archives
Misconduct and disciplinary records – Allegations of student misconduct confirmed under the Student Conduct Rule	FDA1-02	Retain for 14 years after action complete (penalty imposed)
Misconduct and disciplinary records – Other grievance, misconduct and disciplinary records not considered under the Student Conduct Rule	GA47-1.5.2	Retain minimum of 7 years after action completed
Register of recipients of awards, prizes and scholarships	GA47-1.3.2	Required as State archives
Records relating to the accreditation of the institution	GA47-4.3.1	Required as State archives
Research		
Research ethics – Human	GA47-3.4.1	Retain minimum of 15 years after action completed
Research ethics – Animal	GA47-3.4.2	Retain minimum of 7 years after action completed
Research ethics – Biosafety	GA47-3.4.3	Retain minimum of 10 years after action completed
Research data created as part of research activities which are of regulatory or community significance	GA47-3.5.1	Required as State archives

Research data created as part of research activities from clinical trials, or research with potential long-term effects on humans, which are not of regulatory or community significance	GA47-3.5.2	Retain minimum of 15 years after completion of research activity or until subject reaches or would have reached the age of 25 years, whichever is longer
Research data created as part of research activities which do not involve clinical trials, research with potential long-term effects on humans, gene therapy or which are not of regulatory or community significance	GA47-3.5.3	Retain minimum of 5 years after project completed
Research final reports	GA47-3.4.4	Required as State archives
Research grant applications/revenue	GA47-3.3.2	Retain minimum of 7 years after all conditions of the grant have been satisfied
Human Resources		
Employment summary, records summarising the employment or service history of personnel Incudes: name, date of birth, dates of employment/service, positions held and salary, locations worked	GA28-15.4.1	Required as State archives
Workers compensation – Incident has resulted in serious personal injury or incapacity	GA28-3.2.1	Retain minimum of 75 years after date of birth or minimum of 7 years after employment ceases, whichever is longer
Workers compensation – Incident has not resulted in death, serious personal injury or incapacity	GA28-3.2.3	Retain minimum of 25 years after action completed
Personnel / employee files – records documenting the appointment and subsequent employment history (including separation) of employees	GA28-15.4.3	Retain minimum of 75 years after date of birth or minimum of 7 years after employment ceases, whichever is longer
Records documenting the selection and appointment of Chancellors and Vice Chancellors	GA28-15.4.2	Required as State archives
Safety inspections concerning hazardous substances	GA28-14.6.1	Retain minimum of 75 years after action completed
Safety inspections concerning work health and safety risks or hazards	GA28-14.6.2	Retain minimum of 7 years after action completed
Occupational health and safety accidents – Incidents that result in serious personal injury or incapacity to employees	GA28-14.1.1	Retain minimum of 75 years after action completed

Occupational health and safety accidents – Incidents involving employees that do not result in death, serious personal injury or incapacity to employees	GA28-14.1.3	Retain minimum of 25 years after action completed
Occupational health and safety accidents – Incidents involving members of the public, including work experience students and volunteers or other persons who are not employees	GA28-14.1.4	Retain minimum of 15 years after action completed or until expiry of statutory limitation periods, whichever is longer
Type of records		**Retention requirements**
Medical records	GDA17-1.1.3	Retain minimum of 7 years after last attendance, official contact, or access by or on behalf of the client or until patient attains or would have attained the age of 25 years, whichever is longer
Financial Management		
Financial accounting records documenting the organisation's financial transactions. Includes revenue, expenditure, debt recovery and deposits	GA28-7.1.1	Retain minimum of 7 years after end of financial year in which transaction was completed
Treasury management strategy	GA28-7.19.1	Required as State archives
Budgets estimates, including estimates for expenditure, and supporting documents prepared for external approval, e.g. by the organisation's parent department or Minister. Includes variations on estimates	GA28-7.8.1	Required as State archives
Budget estimate records relating to the development and review of budget estimates, including supporting documents prepared for internal use	GA28-7.8.2	Retain minimum of 6 years after preparation
Contracts	GA28-4.0.1	**(A) For specialty contracts (made under seal)**: Retain minimum of 12 years after expiry or termination of agreement or after action completed, whichever is later **(B) For standard contracts or agreements**: Retain minimum of 7 years after expiry or termination of agreement or after action completed, whichever is later
Commercial Activities and Services	GA47-6.0.1	Retain a minimum of 7 years after provision of services ceases or minimum of 7 years after all conditions of contract are satisfied, whichever is longer

Facilities Management		
Asset registers	GA28-7.5.1	Retain minimum of 7 years after asset is disposed of, or minimum of 7 years after data has become obsolete
Lease agreements where the University is the lessee	GA28-16.14.1	Retain minimum of 7 years after lease expires or is terminated
Lease agreements where the University is the lessor	GA28-16.15.1	Retain minimum of 7 years after lease expires or is terminated
Lease agreements for long term leasing-out of land and property, such as perpetual and 99 year leases	GA28-16.15.3	Required as State archive
Maintenance history of a building relating to major maintenance work carried out during the lifetime of a building	GA28-16.16.1	Retain until property is disposed of, then destroy or transfer to new owner as required
CCTV footage	GA28-16.24.7	Usually kept for 30 days unless required for evidentiary, regulatory or other operational purposes
Hazardous material management, including asbestos used or encountered in construction work	GA28-16.7.5	Retain minimum of 75 years after removal or disposal of hazardous materials, then destroy OR transfer to new owners on disposal of property
Governance		
Committees – Inter-government, records relating to inter-government committees where the University provides the State representative	GA28-1.0.2	Required as State archives
Committees – Inter-agency/external, records relating to inter-agency or external committees where (1) the University provides the secretariat and (2) the committee was established for the purposes of strategic planning or policy development and considers issues impacting on the core functions or responsibilities of the University	GA28-1.0.3	Required as State archives
Committees – Inter-agency/external, records relating to inter-agency or external committees where (1) the University does not provide the secretariat or (2) where the University provides the secretariat but the committee considers operational matters or matters relating to administrative or non-core functions of the organisation	GA28-1.0.4	Retain minimum of 5 years after action completed

Committees – Internal, records relating to internal committees established for strategic planning or policy development purposes which consider significant issues impacting on the core functions or responsibilities of the University	GA28-1.0.5	Required as State archives
Committees – Internal, records relating to internal committees which form part of consultative arrangements with staff regarding working conditions e.g. occupational health and safety committees	GA28-1.0.6	Retain minimum of 10 years after action completed
Committees – Internal, records relating to internal committees which consider operational matters and issues concerning the administrative or general operational support functions of the organisation	GA28-1.0.7	Retain minimum of 5 years after action completed
Committees – Advisory / consultative, records relating to meetings of advisory or consultative committees, councils etc. i.e. committees consisting of external stakeholder representation, which advise on or oversee the operations of, or delivery of services	GA28-1.0.8	Required as State archives
Legal advice concerning significant matters	GA28-13.1.1	Required as State archives
Legal advice concerning matters not considered significant	GA28-13.1.2	Retain minimum of 15 years after action completed
Legal litigation records concerning significant matters	GA28-13.4.1	Required as State archives
Legal litigation records concerning matters not considered significant	GA28-13.4.2	Retain minimum of 7 years after action completed
University's copyright agreements	GA28-19.1.2	Retain minimum of 70 years after date of agreement, or after expiry date specified in agreement
Intellectual property	GA28-19.10.1	Retain minimum of 5 years after intellectual property rights lapse
Annual reports	GA28-10.11.1	Required as State archives

Strategic management plans – High level planning of core business functions, activities, projects, programs and services. Includes approved versions of strategic, corporate, or business plans applying to the University as a whole	GA28-19.14.1	Required as State archives
Strategic management plans – Development and review of the University's strategic, corporate or business plans	GA28-19.14.2	Retain minimum of 7 years after plan is superseded
Strategic management plans – Plans and strategies for providing ongoing administrative or operational support	GA28-19.14.3	Retain minimum of 7 years after plan is superseded
Establishment restructuring records relating to the establishment of new organisational structures, or to the review of existing structures and programs which result in significant changes to core functional areas or the organisation as a whole	GA28-6.6.1	Required as State archives
Software licenses	GA28-20.2.1	Retain minimum of 7 years after expiry or termination of agreement or minimum of 7 years after action completed, whichever is longer
Policy and procedure – Final approved versions of by-laws and rules (including final approved versions of strategic policies governing core functions such as teaching, research and admissions)	GA47-4.1.1	Required as State archives
Policy and procedure – Records relating to the development and review of strategic or high-level policies governing core functions	GA28-19.15.3	Required as State archives
Policy and procedure – Final approved versions of University-wide or cross-functional policies concerning operational matters and University-wide or cross-functional procedures	GA47-4.1.2	Retain minimum of 15 years after superseded

Policy and procedure – Records relating to the development and review of by-laws, rules, University-wide or cross-functional policies concerning operational matters and University-wide or cross-functional procedures	GA47-4.1.2	Retain minimum of 15 years after superseded
Policy and Procedure – Final approved versions of local procedures, manuals etc. developed by business units to facilitate day-to-day operations	GA28-19.16.1	Retain minimum of 5 years after superseded
Policy and procedure – Records relating to the development and review of local procedures, manuals etc. developed by business units to facilitate day-to-day operations	GA47-4.1.3	Retain until administrative or reference use ceases

State archives are kept as permanent records of the State of NSW

For further details relating to specific retention requirements for other records contact records@newcastle.edu.au