## **­Purpose**

The purpose of this guide is to assist System and Information Owners 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 high value records require more rigorous management processes, whereas the low-risk low value records have more flexibility in their record management provided that key recordkeeping and privacy obligations are met.

## **Scope**

This guide applies to University records that are subject to and defined by the [Records and Information Management Policy](https://policies.newcastle.edu.au/document/view-current.php?id=81).

This guide should be read in conjunction with the [Information Security Data Classification and Handling Manual](https://policies.newcastle.edu.au/document/view-current.php?id=256) which outlines how the sensitivity of records and information is used to determine the controls required to protect them.

#### Definition

* 1. “high risk records” means those University Records, information and data that are created or received in high-risk areas of the business, or high-risk business processes or functions that would be considered at a level of risk that is outside the University’s risk appetite if they were misused, released inappropriately or inappropriately accessed and altered, lost, damaged or destroyed prematurely. They are required to carry out core functions, to make key decisions and to give evidence of those key decisions at a later date: it demonstrates the performance of legislated functions, the interactions with and entitlements of students, clients and employees.
	2. “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;

Examples of records that are considered to be high risk 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, universities 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,
* rights, entitlements, wellbeing, responsibilities. For example, student and staff related policies, Rules and by-laws,
* 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, 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 Framewor](https://policies.newcastle.edu.au/document/view-current.php?id=274)k.

#### 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.

#### Additional risk considerations also include:

* Where records are held: for example, whether the 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.

#### 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 the longer the retention period. For example, digital 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.

An example of risk mitigation would be to store records and information that have longer retention requirements in the University Record Management system, or to store physical records in an approved University storage location.

## **How to apply risk levels to records**

#### Use Table 1 - Data Classification table to classify the records and information you are responsible for. Table 2 provides examples of the likely business impact/ consequences if records are lost, inaccessible, incomplete, or subject to unauthorised access, modification, or disclosure. Use the highest severity where there is a mix of records with different risk ratings.

#### Identify the retention requirements utilising the *Disposal Authorities* that are located on the[University’s Records Governance web page,](https://www.newcastle.edu.au/current-staff/our-organisation/governance/legislation-and-compliance/records-governance/record-retention-and-disposal) or the examples provided in Table 3 (appendix 1).

#### Once you have identified the retention requirements and the data classification for your records, use the Record Risk Matrix below to identify the level of risk that applies to the records you are responsible for.

#### Implement the necessary record controls (5.1 below) to manage the risks.

## **Table 1. Data Classification Table**

**Use this table to classify your information**

|  |  |
| --- | --- |
| **Impact Type** | **Severity** |
|  | **Lowest Highest** |
| **Impact / Consequence** | **Insignificant or Minor** | **Moderate** | **Major** | **Severe** |
| Security – What competitive advantage does this information provide | Little or no advantage | Might provide some advantage | Definite advantage | Significant Advantage |
| Likelihood of the competitors looking for this information. | Low or no possibility | Low Possibility | Medium Possibility | High Possibility |
| **DATA CLASSIFICATION**  | **Consider for PUBLIC OR UNCLASSIFIED** | **Consider for X – In Confidence** | **Consider for Restricted** | **Consider for HIGHLY Restricted** |

## **Table 2 – Example of consequences if information became inaccessible, incomplete, or subject to unauthorised access, disclosure, or modification**

|  |  |
| --- | --- |
| **Impact Type** | **Severity** |
| **Impact** | **Insignificant or Minor** | **Moderate** | **Major** | **Severe** |
| **General / Provision of business operation and service**.**For example,** loss/inaccessible research data stored on a hard drive of an unsupported computer resulting in an inability to meet contracted reporting obligations for research grants, or the loss of evidence relating to intellectual property. | * 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.

Existence of the University under threat. |
| **Compliance / Legal****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 does not have any penalty or litigation impact.
* 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.
* No litigation or prosecution and/or penalty.
* Regulatory consequence limited to standard inquiries.
 | * 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.
 |
| **Employees / WHS****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. | * 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 serious injury, or negative environmental impact, and the relevant external authority 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/or senior staff.
 |
| **Financial****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** **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. | * 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.
* Serious public outcry and/or international coverage.
* 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’s teaching, research and/or business functions.
* Loss of one full day of teaching, research and/or business functions.
 | * Loss of 1-7 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.
* Course catalogues.
* Published research data.
* Course descriptions.
 | * Business unit process and procedure.
* Unpublished intellectual property.
* ITC system design and configuration information.
* 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 information.
* 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 rities**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Impact / Consequences** | **Insignificant** | **Minor** | **Moderate** | **Major** | **Severe** |
| **50 years +**  | **Low** | **Medium** | **High** | **Extreme** | **Extreme** |
| **11-20 years** | **Low** | **Medium** | **Medium** | **High** | **Extreme** |
| **8-10 years**  | **Low** | **Low** | **Medium** | **Medium** | **High** |
| **1-7 years** | **Minimal** | **Low** | **Low** | **Medium** | **Medium** |

#### 5.1 Record controls:

1. For records with a **low or minimal** risk level there may be flexibility in how records are managed providing key recordkeeping obligations are still met, including protecting State Archives (and 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**.**
2. For records with a **medium** risk level, reasonable records management practices need to be in place and the records must be captured formally into the University approved Records Management System.
3. 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 University Records Governance Service to determine the 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.

**Refer to the** [**Information Security Data Classification and Data Handling Manual**](https://policies.newcastle.edu.au/document/view-current.php?id=256) **for further controls that need to be applied to records and information to mitigate risk.**

#### Appendix 1

#### Table 3 – Examples of minimum legal retention requirements for university records

|  |  |
| --- | --- |
| **Type of records** | **Retention requirements** |
| **Teaching**  |
| Student administration records | Retain minimum of 7 years after completion or discontinuation of course or program of study by student |
| Professional placement reports  | Retain minimum of 50 years after completion of course of study |
| Final results obtained by student  | Retain minimum of 75 years after action completed |
| Final approved curricula | Required as State Archives |
| Master exams  | Retain minimum of 15 years after superseded |
| Register of graduates/records confirming award/receipt of a qualification | Required as State Archives |
| Misconduct and disciplinary records | Retain minimum of 14 years after action completed |
| Register of recipients of awards, prizes and scholarships | Required as State Archives |
| Records relating to the accreditation of the institution | Required as State Archives |
| **Research**  |
| Research Ethics  | Retain minimum of 15 years after action completed |
| Research data | 5 years, 15 years or Required as State Archives depending on the type of research and whether it is of national or international significance  |
| Research final reports  | Required as State Archives |
| Research grant applications/revenue | Retain minimum of 7 years after all conditions of the grant have been satisfied |
| **Human resources**  |
| Employment summary | Required as State Archives |
| Workers Compensation  | Retain minimum of 75 years after date of birth or minimum of 7 years after employment ceases, whichever is longer |
| Employee records | Retain minimum of 75 years after date of birth or minimum of 7 years after employment ceases, whichever is longer |
| Employee records of the Chancellors and Vice Chancellors | Required to be retained as State Archives |
| Safety inspections | Retain minimum of 75 years after action completed |
| Occupational Health and Safety – accidents | Retain minimum of 25 years after action completed |
| Medical records | 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 | Retain minimum of 7 years after end of financial year in which |
| Records relating to the organisation's Treasury management strategy. | Required as State archives |
| Budgets  | Budget 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 – Required as State Archives |
| Contracts | Retain minimum of 12 years after expiry or termination of agreement or after action completed, whichever is later |
| Commercial Activities and Services  | Retain minimum of 7 years after provision of services ceases or minimum of 7 years after all terms and conditions of contract are satisfied, whichever is longer |
| **Facilities Management**  |
| Asset registers  | Retain minimum of 7 years after asset is disposed of |
| Lease agreements | Retain minimum of 7 years after lease expires or is terminated |
| Building plans, maintenance and conservation records | Retain until property is disposed of, then destroy or transfer to new owner as required |
| CCTV footage  | Usually kept for 30 days unless required for evidentiary, regulatory or other operational purposes |
| Hazardous material management (asbestos records)  | Retain for 75 years after removal or disposal of hazardous material  |
| **Governance** |  |
| Committee records | High level Committees – Required to be retained as State archives. Other committee records need to be retained for 5 – 10 years. |
| Legal records  | Varies – retain for 15 years to State Archives |
| University’s copyright ownership/ agreement | Retain minimum of 70 years after date of agreement, or after expiry date specified in agreement |
| Intellectual Property  | Retain minimum of 5 years after intellectual property rights lapse |
| Annual reports | Required as State archives |
| Strategic management plans  | Required as State archives |
| Establishment restructuring records | Required as State archives |
| Software Licenses | Retain minimum of 7 years after expiry or termination of agreement  |
| Policies, procedures rules and by-laws  | Final, approved versions of by-laws, rules and policies core functions such as teaching, research and admissions where these are not captured in by-laws, rules or minutes of governing bodies – Required as State Archives |

*State Archives are retained as permanent records of the State of NSW*

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