Record Security Guideline

Version	Approved by	Approval date	Effective date	Next full review
1.0	Manager, Records & Archives	13 December 2017	13 December 2017	December 2020

Guideline Statement

Purpose	This guideline details the requirements for security when capturing, accessing and managing University records.	
Scope	This guideline details the requirements for University records captured to RAMS (the Records & Archives Management System)	
Are Local Documents on this subject permitted?	☒ Yes, however Local Documents must be consistent with this University-wide Document.	□ No

Guideline

Contents

1. Introduction

The *Recordkeeping Policy* contains principles that ensure that information in the form of records is discoverable across our organisation by those with legitimate need, whilst our systems protect information from unauthorised access, alteration, deletion or misuse.

The University values its records and information and, through the capture of records to appropriate business systems, the appropriate security requirements may be applied to ensure records and information are made available only to those University staff who require access in the conduct of their duties.

This guideline details the requirements for University records captured to RAMS (the Records & Archives Management System.)

2. Security Framework

All staff are bound by the University's *Code of Conduct* to use the University's systems and resources only in the conduct of their official duties.

All records captured to RAMS acquire the fundamental level of security applied to all of the University's business systems. Only University staff may log into the system using their staff credentials, and audit logs are generated to monitor system usage and ensure all activity is in line with business need.

This basic level of security, previously known as *Unrestricted*, is now inferred by the capture of any record to RAMS.

Further security restriction in RAMS is always applied at the container level. All records captured to a container inherit the security of their container. This enables straightforward administration of security and of record capture. It means that a container and its contents may be both viewed and accessed, or may not.

Additional security may be applied to records where there is a need to further restrict access within the University community. There are three primary means of applying security to RAMS records:

- Security Levels
- Security Caveats
- Access Controls.

Access Control provides the primary means of restricting digital records in RAMS.

Security Levels and Security Caveats are applied only by Records and Archives staff to specific hardcopy records captured in RAMS (refer to Appendix A).

This guideline provides details of these three security methods, including when they are used, and how to apply them.

3. Current Security Controls

3.1. Access Control

Access Control is an opt-in method of specifying access rights to electronic records captured using RAMS. It provides the primary means by which to control access to a University record.

Access Control is applied at a container-level on the attributes *View Document*, *View Metadata* only. This means a staff member will either be able to locate and view the container and its records, or they will not.

More granular control over update rights, modification, contribution etc. are available using Access Control but these are only used in exceptional circumstances due to the excessive administration required to maintain them.

Access Control is applied based on pre-defined Groups within RAMS; GROUP: [*Name of Group*])

Membership of any Access Control Group is based on Position or Unit to ensure membership of the Group is maintained over time through organisational change.

These predefined Groups are maintained by Records and Archives and can be created/updated on request. All Access Groups contain the administrative group, GROUP: Records, to enable Records & Archives staff to maintain access to records at all times solely for the purpose of record administration.

A sample partial cross-section of a RAMS Access Group:

- **GROUP: Heads of School**
- Head, School of Accounting
  - Doe, Jane (Professor)
- Head, School of Aviation
- Head, School of Chemistry
  <…>
- GROUP: Records
  - Records & Archives

4. Legacy Security Controls

4.1. Security Levels

Security Levels provided the primary method for restricting access to hardcopy University records. Any document has an inherent level of security based on its content. Any container would inherit the security level of its most restricted content, as would all other records within the same container.

To view records of a certain security level, a staff member is required to have the same, or a higher level of security applied to their profile.

The Security Levels, in increasing order of restriction, are in *Table 1*.

Table 1: UNSW Security Levels

Security Level	Scope Notes	UNSW Data Classification equivalent*
Restricted	The Restricted classification is for those records documenting staff grievances, privacy issues, FOI requests and legal advice. Information which could: • Compromise Legal professional privilege • Breach staff confidentiality in the complaint resolution procedure. • Compromise information provided under Freedom of Information requests.	Private
Protected	The Protected classification is for those records that relate to Audit requirements. Information which could: • Substantially undermine the financial viability of UNSW. • Facilitate the commission of serious crime; • Seriously impede the development or operation of UNSW and major Government policies.	Sensitive
Highly Protected	The Highly Protected classification is for those records that relate to the governance of the University, industrial relations matters, controlled entities and commercial research ventures and highly sensitive commercial business documents or contracts. Information which could: • Threaten life directly; • Seriously prejudice public order; • Substantially damage the University or state or national finances or economic and commercial interest.	Highly Sensitive

* Refer to the UNSW *Data Classification Standard*

4.2. Security Caveats

Security Caveats provided a secondary means for the restriction of hardcopy records. The Security Caveats that may be applied to hardcopy records are in *Table 2*. They enable a container to be restricted to a specific subset of staff based on role, such as limiting access to Human Resources (HR) records to HR staff only.

Their primary use at UNSW is for the control of access to hardcopy legal, personnel and student records.

A security caveat may be applied with a Security Level, and a user seeking access to the record would be required to meet both sets of criteria (Security Level, Security Caveat) to locate and to view the container.

All staff members receive automated access to relevant Security Levels and Caveats based on their position. Any staff member wishing to confirm their access may contact records@unsw.edu.au for further information.

Table 2: UNSW Security Caveats

Security Caveat	Acronym	Scope Notes
Commercial-in-Confidence	CIC	For hardcopy commercially sensitive records only
Governance-in-Confidence	GIC	For hardcopy records of UNSW Council, Academic Board and associated Committees only
Legal-in-Confidence	LIC	For hardcopy Legal Files only
Personnel-in-Confidence	PIC	For hardcopy Personnel files only
Security-in-Confidence	SIC	For hardcopy security-related files only
Student-in-Confidence	STIC	For hardcopy Student files only

5. Applying and Managing Security

5.1. Applying Access Control

Access Control provides the primary means of restriction of digital RAMS records. Staff creating RAMS containers should consider if restriction of the material to be captured is necessary and, if so, to which areas of the University.

If an existing Access Group exists that provides the required level of restriction, the staff member may apply it themselves whilst creating the container in RAMS.

If no such Group exists, a request must be made to Records & Archives staff who will create the Group as required. To request the creation of an Access Group please contact records@unsw.edu.au to discuss your requirements.

Any Access Group must contain at least three positions or a single Unit, to restrict records further limits their capability as retrievable, useable information.

The Access Control permissions available in RAMS are detailed in *Table 3*.

Table 3: UNSW Access Control

In Use	Access Control	Description
Yes	View Document	Access to open documents within the container and read them.
Yes	View Metadata	Access to view the Metadata of the record, such as the Title. This grants permission to locate the record when conducting a search.
No	Update Document	Access to make changes to the content of a document. Update Document is dependent on View Document access to open the document.
No	Update Record Metadata	Access to update the metadata. View Metadata access is still required to be able to view the metadata.
No	Modify Record Access	Access to set/modify Access Control.
No	Contribute Contents	Access to add new documents to the container.

The use of *Update Document*, *Update Record Metadata*, *Modify Record Access* and *Contribute Contents* can be provided on request, though is generally not recommended due to the additional administrative complexity their application can impart.

View Document and *View Metadata* govern access to the informational content of the record and are required for the other permissions to be available. For example, a document must be retrievable (View Metadata) to be accessible, then a document must be readable (View Document) before it can be edited (Update Document).

All available Access Groups may be located within RAMS by searching the *Locations Directory* with the prefix *GROUP: **

5.2. Applying Security Levels

Security Levels are only applied to hardcopy University records captured in RAMS and, as such, are only applied by Records & Archives staff based on identified requirements.

Staff may request a search of any required topic/keyword by Records & Archives staff. Where records are identified that have a higher level of Security Level restriction than the staff member searching, Records & Archives staff will consult with the record owner on the preferred course of action. Access to restricted material will never be provided without the authority of the record owner.

5.3. Applying Security Caveats

Security Caveats are only applied to hardcopy University records captured in RAMS and, as such, are only applied by Records and Archives staff based on identified requirements.

Staff may request a search of any required topic/keyword by Records & Archives staff. Where records are identified that have a Security Caveat the staff member searching does not possess, Records & Archives staff will consult with the record owner on the preferred course of action. Access to restricted material will never be provided without the authority of the record owner.

Accountabilities	
Responsible Officer	Manager, Records & Archives
Contact Officer	Information Management Analyst, Records & Archives
Supporting Information	
Legislative Compliance	This Procedure supports the University's compliance with the following legislation: *State Records Act, 1998* (NSW) *Evidence Act, 1995* (NSW) *Government Information (Public Access) Act, 2009* (NSW) *Health Records and Information Privacy Act, 2002* (NSW) *Privacy and Personal Information Protection Act, 1998* (NSW) *Children and Young Persons (Care And Protection) Act, 1998* (NSW) *Public Finance and Audit Act, 1983* (NSW) *University of New South Wales Act, 1989* (NSW) *Work Health and Safety Act, 2011*
Parent Document (Policy and Procedure)	Recordkeeping Policy Recordkeeping Standard

Supporting Documents	Record Titling Guideline Archives Access Guideline Archives Acquisition Guideline
Related Documents	Data Governance Policy Data Classification Standard Email Policy IT Security Policy Procurement Policy
Superseded Documents	Nil
File Number	2017/25742

Definitions and Acronyms

Archive	A Record that the University has committed to retaining permanently for either the maintenance of a permanent record of the activities of the State of NSW (State Archives) and/or as a cultural, historical record of the University (University Archives.)
Appraisal	The process of assessing records to determine the period of time for which they must be retained prior to destruction or deletion, or preservation in an archive.
Record	Any recorded information made or received by a staff member of the university in the course of undertaking their duties. Records are evidence or information about university activities. They can be any format.
RAMS	Records & Archives Management System. The University's corporate recordkeeping system, previously known as TRIM.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Manager, Records & Archives	13 December 2017	13 December 2017	This is a new procedure

Appendix A: Security Framework Summary

Security Type	Notes	Still in Use?
Security Levels	Defined by content of record, hierarchical structure, aligned to UNSW Data Classification scheme	Only for Legal records, and specific activities related to information management (i.e.; GIPA requests)
Security Caveats	Defined by staff role, restrict record content to specific Caveat. Can be used in combination with Security Levels to increase restriction	Only Legal, Personnel and Student records.
Access Groups	Pre-defined Groupings of Units/Positions based on business activity. Access restricted to membership of the Group only.	Yes