Records Management - Security of Records Procedure

Section 1 - Purpose / Objectives

(1) Many records held by Victoria University (VU) contain sensitive information, particularly personal information and commercial-in-confidence information. VU needs to be able to protect this information from inappropriate access, while also allowing sufficient access to enable staff to carry out their functions. These procedures outline how access to records is controlled within VU, and how security is maintained to protect against inadvertent release.

Section 2 - Scope / Application

(2) This procedure applies to:

a. all University staff and contractors, council members, honorary, adjunct or visiting academics, and volunteers; and
b. all records (both physical and electronic) created or held by VU, or created or held by contractors on VU's behalf.

Section 3 - Definitions

(3) Nil

Section 4 - Policy Statement

(4) Nil

Section 5 - Procedures

Roles/Responsibilities

Roles	Responsibility
All VU staff, contractors, Council members and visiting teachers	a. Responsible for determining security classification levels for the records they create.
Managers	a. Responsible for identifying categories of records that are created in their unit that should have a default classification of Open or Restricted. b. Responsible for determining who is able to access Restricted records created within their unit.

Security Classification

(5) Every record must have a security classification, which determines who is able to access the record, and what level of security it requires. The security classification levels, and the process for determining a classification level, are outlined below.

Security classification levels

(6) There are three security classifications which can be applied to records:

a. Restricted	Records that contain information which could damage the interests of individuals or organisations (including students, staff, VU, and third parties) if it is disclosed to the wrong person, must be classified as Restricted. Records containing personal information, commercially sensitive information, legal advice or opinions, and information communicated in confidence must be classified as Restricted. Restricted records must only be made available to staff with a clear business need to access the information, in accordance with these procedures.
b. Internal	Records that may contain some low level sensitive information, or where sensitivity has not been properly assessed, should be classified as Internal. Internal records can be freely circulated within VU (ie to VU staff or contractors) but should not be released to students or third parties outside VU, except in accordance with these procedures. This is the default classification level that should be used for records that have not been assessed as falling into one of the other classifications.
c. Open	Records that do not contain any sensitive information should be classified as Open. Open records have been cleared for release outside VU, including to the media, students or the general public. Open records may still contain copyright material, so although they can be accessed by anyone there may be restrictions around copying or re-use.

Determining classification levels

(7) Staff should apply a security classification level to records when they are created. The default classification for records is Internal. Managers should identify categories of records that are created in their unit, which should have a default classification of either Open or Restricted. For example, the default classification for media releases would be Open, while for student records it would be Restricted. In most cases staff will simply confirm the default classification when they create a record.

(8) Staff should consult with their manager if they are in doubt about the classification level that should be applied to a record.

(9) Examples of different classification levels:

a. Restricted	i. Student records ii. Research data on identified individuals iii. Commercially sensitive research records iv. Staff records v. Legal advice vi. Complaints and grievances
b. Internal	i. Planning records ii. General correspondence with external organizations iii. Internal communications
c. Open	i. Media releases ii. Current marketing material iii. University policies

Process for classifying records:

(10) See flow chart on process for classifying records.

(11) The Records Classification Checklist [insert link] can be used to determine the classification level for a group of records.

Recording classification levels

(12) Physical records should be marked with their classification, using a stamp, electronic watermark or header, or

pre-printed file cover. Where records have not been labelled it should be assumed that no classification decision has been made, and hence they may contain material properly classified as Restricted.

(13) For electronic records, electronic watermarks or headers can be used to mark records with their classification.

(14) In some cases records exist within electronic systems, and it is possible to apply a single classification to the entire system. For example, all records within VU Connect are classified as Restricted. In other cases the system will allow a classification level to be recorded against each individual record within the system. For example, records in RecFind have a security code which reflects the classification level of the records.

Classifying legacy records

(15) Legacy records which pre-date these procedures will normally be unclassified. Records which are labelled with older access statements (such as "Confidential", "Legally Privileged" etc.) should be regarded as Restricted.

(16) The Records Classification Checklist [insert link] can be used to classify groups of legacy records. Legacy records should be classified whenever it is practical to do so.

Re-classifying records

(17) Records can be re-classified at any time if the sensitivity of the information in the record changes.

(18) Staff should only lower the classification level on a record (i.e. change a classification from Restricted to Internal, or from Internal to Open) in consultation with their manager.

Determining access to restricted records

(19) Access to Restricted records is based on the "need to know" principle. In other words, Restricted records should only be accessed by staff with a clear business need to access them (i.e. a "need to know"). Managers should identify the categories of Restricted records that are created within their business unit, and determine who should be able to access each category of records.

(20) For example, a college may create the following categories of Restricted records:

a. Records containing students' personal information;
b. Records containing personal information on staff members;
c. Commercially sensitive records relating to a research project involving a partnership with a private company; and
d. Research data on individuals collected as part of several research projects.

(21) The staff who would need access to the Restricted records would be different for each category of Restricted records. There would be a very limited number who have access to records containing personal information on staff, while Restricted research records should only be available to staff who are working on that research project.

(22) Folders in the shared network (Y:) drive must have security controls to prevent inappropriate access. The manager should determine the security groups that should have access to each folder containing Restricted records, and arrange for ITS to implement appropriate security controls. The security groups should be documented in a register kept by the business unit, and kept up to date as staff change. At least once a year, the manager should ask ITS for a list of who has access to the folders in their Y: drive, and check this against the register to identify any discrepancies.

(23) Do not use password protection to restrict access to electronic documents stored on the Y: drive. Passwords are easily lost or forgotten, which may prevent authorised users from accessing the documents.

(24) Where an electronic system contains Restricted records, access to the system should only be given to those staff that require it for their work. The manager who is responsible for the system should ensure that there is a process in place to regularly review who has access to the system, to ensure that staff who change roles are not retaining access to the system if they no longer require it. If possible, the system should allow different permissions to be granted to each user, so that each staff member only has access to the records that are relevant to their work, rather than all records within the system. In this case, logical security groups should be identified based on the work that staff do, and permissions should be developed for each security group.

(25) There will also be times when staff outside the business unit require access to Restricted records. Access should be provided in consultation with the manager of the business unit, or in accordance with guidelines established by the manager.

(26) When granting a staff member access to a Restricted record, the following questions should be considered:

a. Why does the staff member need to access the record? Is this a legitimate business reason?
b. Could the business need be met by providing non-sensitive information from the record?
c. Is it possible to provide only part of the record? For example, the record could be photocopied with the sensitive information covered or obscured.

Access by contractors

(27) All contractors who may have access to Internal or Restricted records must have signed a confidentiality agreement, or have a confidentiality clause as part of their contract. A standard confidentiality agreement is available from Legal Services. Managers or staff who are working with contractors must make sure they are aware which records are confidential, and that they understand appropriate procedures for handling confidential records (see Guidelines for Handling Restricted Records [insert link]).

Security of Records

(28) Please refer to the ITS Security Policy [insert link] for direction on maintaining the security of electronic information.

Records classified "internal"

(29) All records must be stored in an area that is only accessible to staff, or is under constant supervision by staff when accessible to members of the public (see Procedures for Storage of Physical Records [insert link]). Records should not be left where they can be viewed by members of the public.

(30) When moving records (eg during an office relocation) records must not be left unattended. Removal contractors must have appropriate procedures in place to ensure this does not happen. Thorough checks should be undertaken to ensure that records are not left behind during the move.

(31) Records must be destroyed securely (see Records Disposal Procedures [insert link]).

Records classified "restricted"

(32) Restricted records must be stored in an area that is only accessible to those staff who are authorized to view the records (see Procedures for Storage of Physical Records [insert link]). This may mean a locked filing cabinet, a locked compactus, or a locked store room. Keys or fob access should be provided to authorized staff only. The business unit should keep a register of staff with key or fob access.

(33) If the storage area is secured by fob access, then the manager must notify Facilities when staff change. At least once a year, the manager should ask Facilities for a list of who has fob access to the secure area, and check this

against the register to identify any discrepancies.

(34) When moving records (e.g. during an office relocation) records must not be left unattended. Removal contractors must have appropriate procedures in place to ensure this does not happen. Thorough checks should be undertaken to ensure that records are not left behind during the move.

(35) Records must be destroyed securely (see Records Disposal Procedures [insert link]).

Section 6 - Guidelines

(36) Nil

Status and Details

Status	Historic
Effective Date	19th August 2014
Review Date	19th April 2017
Approval Authority	Vice-Chancellor
Approval Date	19th August 2014
Expiry Date	11th July 2016
Responsible Officer	Ana Mitrovic Manager, Records and Archives Services +61 3 99199553
Enquiries Contact	Ana Mitrovic Manager, Records and Archives Services +61 3 99199553