Information Security Classification Policy and Procedures

1. PURPOSE

The University recognises that its corporate information is an important strategic asset. The *Information Security Classification Policy* aims to establish and maintain a framework for assessing the sensitivity and importance of its corporate information.

2. APPLICATION

All Staff and Students

University Associates

Organisations or people performing outsourced services on behalf of Curtin University of Technology

Regional and offshore campuses and offices of Curtin University of Technology

Volunteers performing duties or services for Curtin University of Technology

3. EXCEPTIONS

Nil

4. DEFINITIONS

(*Note:* Commonly defined terms are located in the *Curtin Common Definitions*. Any defined terms below are specific to this document)

Information Security Classification
A process where the creator of University Information assesses the sensitivity and importance of the information and assigns a label to the information so that it can be managed or stored with consideration to its sensitivity and importance.

Protective Marking
A physical or electronic label attached to information to indicate the Security Classification that is assigned.

University Information
Is any information irrespective of format created or managed by Curtin staff, associates, contractors, volunteers or students in connection with their employment, business dealings, research or studies at the University.

5. POLICY STATEMENT

All University information must be given an Information Security Classification so that it may be managed and secured in a manner appropriate with its sensitivity and importance.

5.1 Access to University information

The University encourages the sharing of information assets to ensure organisational effectiveness. University staff and students are provided with access to University information in order to effectively carry out their activities. However, where there are confidentiality or privacy requirements, access is restricted to particular staff positions or organisational units according to business and legislative requirements.

5.2 Responsibility

The creator of University Information is responsible for assessing the sensitivity and importance of the information they have created. The creator is also responsible for ensuring that the information is appropriate labelled with a protective marking.

5.3 Documents received from external parties

The recipient of the information is responsible for ensuring that documents received from external parties receive a Security Classification that conforms with the University's *Information Security Classification Policy* if it is to be retained as University information.

5.4 Information Re-classification

The creator or the responsible area may re-classify information if the sensitivity or importance changes, or if the information was incorrectly classified. The protective marking must be amended to indicate the new Security Classification.

5.5 Security Classifications

University Information shall be classified into one of the following classifications:

- Public
- Internal Only
- X-in-Confidence
- Protected

5.5.1 Public

University Information that is publicly available and unlikely to cause harm to the University, another organisation, or an individual. Examples would include prospective students course outlines, the academic calendar and Curtin's public website.

5.5.2 Internal Only

University Information that is generally not publicly available. The release of this information to the general public could cause minor harm to the University, another organisation, or an individual. Examples would include the departmental telephone directory, academic lecture notes, iLectures and Curtin's Intranet.

5.5.3 X-in-Confidence

University Information that must be kept confidential, access is on a need to know basis only. Unauthorised disclosure, modification, or destruction could reasonability be expected to:

- Cause harm to the University, another organisation or an individual; Provide an unfair advantage to an entity; or
- Violate somebody's right to privacy.

The "X" is substituted by subject label that describes the subject matter. The following are authorised X in Confidence protective markings:

Security-in-Confidence	For information that contains details of security measures established to protect people, facilities, assets, or information resources. Eg. Encryption keys and administrator passwords
Staff-in-Confidence	For information that contains private or personal details of Curtin staff or associates. Eg. Personnel files.
Commercial-in-Confidence	For information that contains trade secrets or commercially valuable details about a business. Eg. Commercially sensitive information provided by business/trade partners.
Medical-in-Confidence	For information that contains private medical details about a patient. Eg. Information that would be considered Doctor/Patient privileged information.
Legal-in-Confidence	For information concerning a confidential legal matter that has been communicated between legal counsel and their client. Eg. Legal privileged information.
Student-in-Confidence	For information that contains private or personal details of Curtin students. Eg. Student academic records.

5.5.4 Protected

University Information that must be kept strictly confidential, access to the information must be restricted to only persons who are explicitly granted access to that information. Unauthorised disclosure, modification, or destruction could reasonably be expected to cause:

- Serious harm to the University, another organisation or an individual;
- Compromise Australia's national security;
- Damage Australia's national interests, economy, stability or integrity; or
- Damage Australia's international relations or defence.

5.6 Protective Markings

University information that has been assigned a security classification must be labelled with a protective marking that reflects that classification.

6. OBJECTIVES

To ensure that all University information is assessed to determine its sensitivity and importance.

To appropriately protect and manage the information in accordance with relevant policies and regulatory requirements.

7. PROCEDURES

7.1 Assigning an Information Security Classification

When University information is created the creator must determine the classification of that document based upon the confidentiality, sensitivity and criticality of the information. The Information Classification must be one of the classifications specified in this policy. This also applies to information received from third parties that the receiver intends to retain as University information. For example an academic transcript from another University submitted by a student that is retained on the student's record.

7.2 Default Information Security Classification

Information will be classified as INTERNAL ONLY by default unless reclassified by the responsible area.

7.3 Information Security Classification Guideline

When determining an Information Security Classification, the Information Security Classification guideline should be used (see Schedules).

7.4 Protective Markings

The creator or receiver of University information is responsible for labelling the information. The protective marking may be in the form of:

- The security classification printed on a file cover in UPPERCASE and **BOLD** on the front of the file;
- The security classification appearing in the header or footer of the document in UPPERCASE and **BOLD**, clearly visible to the reader when the document is separated from the system in which it is managed.;
- The security classification printed on removable media in UPPERCASE and **BOLD**;
- The security classification appended to the name of the electronic folder in UPPERCASE and **BOLD.**

In addition to these visible protective markings it is also required that a mandatory metadata field marked "Security Classification" be completed for all electronic information. This metadata field should be visible to all staff who access the electronic information contained within information management systems so that electronic information can be more easily managed.

7.4 Changing or Downgrading Classifications

University information may be re-classified by the responsible area at any time to reflect changes in the information's confidentiality, sensitivity, and criticality. If the information is

re-classified, a new protective marking must be immediately assigned, and any security controls associated with that security classification must also be immediately applied.

University information should have the Security Classification downgraded when protection is no longer necessary or is no longer needed at the original level. Generally, security classifications should be reviewed when information becomes inactive and no longer in regular use. This can be done in conjunction with existing information disposal processes outlined in the *Information Management Procedures*.

Archival information will automatically be downgraded to "Public" once it is 25 years old unless it has been identified as a "Restricted Access Archive" as described in Curtin's *Recordkeeping Policy*.

8. LIST OF SCHEDULES

Schedule A - Information Security Classification Guideline

9. OTHER RELEVANT DOCUMENTS/LINKS

State Records Act 2000

Evidence Act 1906

Freedom of Information Act 1992

Criminal Code 1913

Electronic Transactions Act 1935

Australian/International Records Management Standard ISO/AS 15489

Information Security Management System ISO/IEC AS/NZS 27001

Recordkeeping Policy

Information and Communication Technology (ICT) Policy Manual

Curtin Information Statement

Curtin Recordkeeping Plan (2008)

Information Privacy Principles (under Commonwealth Privacy Act 1988)

Policy Compliance Officer	Robbie Whittome, Manager, IT Security, Risk and Information Management | Curtin Information Technology Services
Policy Manager	Chief Operating Officer
Approval Authority	Planning and Management Committee
Review Date	1st April 2010

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes and Notes
	Approved	28/07/2006	Planning and Management Committee	PMC 79/09	Attachment 2 to Document No 010154/09
	Administratively Updated	15/09/2015	Compliance Consultant		Policy Contact Updated
	Administratively Updated	06/10/2015	Director, Legal and Compliance Services	EC 76/15	Executive Manager Title Changes
	Administratively Updated	18/01/2017	Director, Legal and Compliance Services		Review date updated

Curtin University

Selecting an Appropriate Security Classification