Monash University Procedure

Procedure Title	Electronic Information Security: Responsibilities, Classifications and Standards Procedures
Parent Policy	Electronic Information Security Policy
Date Effective	12-September-2012
Review Date	12-September-2015
Procedure Owner	Chief Information Officer
Category	Operational
Version Number	1.0
Content Enquiries	eSolutions Service Desk
Scope	All campuses in Australia Monash South Africa Monash College Pty Ltd All staff All students
Purpose	The University recognises its responsibility to ensure the security of the electronic information that is used in its activities, including research, education, international and administrative information.
PROCEDURE STATEMENT	

Responsibilities for Securing Electronic Information

1. The Chief Information Officer will consult with University functional areas, and determine Information Owners for administrative, research and education information.
2. In accordance with the Electronic Information Security Policy, the Information Owner will review and define information for their functional area on an annual basis.
3. The Information Owner will promulgate information security classifications, procedures and local business rules for handling data sets for their functions area to Information Custodians and Information Users.
4. The Information Owner will conduct audits to identify critical information and ensure the defined procedures have been followed.
5. The Information Owner will maintain Information Classification Registers for their functional area.
6. The Information Owner will complete an annual return to the Director, Risk and Compliance, certifying that their responsibilities under the Electronic Information Security Policy have been met.
7. Any disputes regarding the appropriate classification of information will be resolved by a panel consisting of the University Privacy Officer, Human Resources Division, and representatives from the University Solicitor's Office, Risk and Compliance and Security and Risk Section, eSolutions.
8. Information Custodians and Information Users are required to consider carefully the information they are working with and to discharge their responsibilities in accordance with the Standards for Data Protection (see below). Custodians and Users must not transfer or store Critical Information in email, Microsoft Word/Excel etc. unless the manner of doing so meets the storage and

transmission requirements stipulated in the Standards for Data Protection. Technical advice can be sought from the Risk and Security section of eSolutions by contacting the IT Service Desk.

9. Any deviation from the Standards for Data Protection will require a waiver in the form of written approval from the Information Owner. The waiver will be recorded on the Information Owner's Information Register.

Responsibility
Those with functional responsibilities cited.

Classifications of Electronic Information

The Information Owner will classify information for their functional area according to the following classification definitions:

Critical: This classification applies to *highly sensitive* information:

- where the access, distribution, retention and/or destruction of information is subject to restrictive regulatory obligations; and
- unauthorised disclosure would seriously and adversely impact the University, its employees, its students and/or its partner organisations; and
- access to this information is strictly limited to a selected group or process.

Critical information is information that, if compromised, would place the University in breach of its legal and regulatory responsibilities.

Examples of **critical information**:

- Credit card numbers: Credit card numbers are a target of internet theft.
- Tax file numbers: Tax file numbers are required by the Australian Tax Office to be stored and used securely. Failure to adopt appropriate measures could see the University in breach of its legal responsibilities.
- Health Information: Health information is highly sensitive and subject to a number of statutory controls, including, but not limited to: the Information Privacy Act and the Health Records Act. The accidental disclosure of health information could result in significant adverse press for the University and fines for breaches of data confidentialy requirements.
- Reportable Police Information (incidents and violations).
- Information classified by Human and Animal Ethics COmmittees.

Protected: This classification applies to *sensitive* information:

- where unauthorised disclosure may adversely impact on the University, its employees, its students and/or its partner organisations; and
- where access is limited to a selected group or process.

Examples of **protected information**:

- Financial information, such as purchase orders. Note: Care must be taken to ensure that financial information is not subject to regulatory compliance requirements and hence classified as Critical. An example is banking details.
- Discipline Committee Meeting Minutes.
- Staff Employment Contracts.
- Student Evaluation of Teaching and Units data.

- Research data set inputs.
- Communications with research partners.

Restricted: This classification applies to *confidential* information:

- that does not include sensitive information, but is created or received within the University (including by students) and used internally; and
- the release of this information would not cause damage to the University, its employees, its students and/or its partner organisations; but
- approval from the Information Owner must be obtained before restricted information can be made public information.

Examples of **restricted information**:

- course materials and content.
- Employment opportunities at Monash (Staff Only).

Public: This classification applies to *publicly available* informationl

- that is made available, or released to the general public; and
- where no adverse effects are expected to result from the wide circulation of this information.

Examples of **public information**:

- The Monash University home page (www.monash.edu.au).
- Faculty course lists and the University Handbook.
- Monash research achievements and broadcast events.

Unclassified: This classification relates to *information that has not been classified*:

- Unclassified information is to be treated as **protected** until classified.

Responsibility
Information Owners

Standards for Data Protection

CLASSIFICATION	ACCESS	USE	STORAGE	TRANSMISSION	DISPOSAL
Critical	Relevant fields must be encrypted using an approved encryption method. Access to records and files must be restricted to specific job	Use is prescribed by the Information Owner and is generally not available outside the Information Owner's domain (exceptions	Information, other than that stored on secondary backup devices, must be stored on non-transportable, non-removable	Information must be encrypted using an approved encryption method when transmitted. Information must not be made available via the Internet, the	Information must be removed before the storage device is retired or reused. If the information cannot be removed, the device must be destroyed.

	roles, and requires authentication and password protection. Repairs to storage devices must be undertaken onsite and under supervision of eSolutions staff.	are Government bodies, financial institutions).	storage devices under the control of eSolutions. Contracts with 3rd party providers must include appropriate Standards for Data Protection and privacy clauses.1[1]	wireless network or by facsimile. Transmission must only be by a dedicated secure link (e.g. DIISRTE, credit card gateway) or transported by hand.	
	Secondary Storage Devices - Backup of Critical Data				
	Relevant fields must be encrypted using an approved encryption method. Record and file access must be password protected. Repairs to secondary storage devices must be undertaken onsite and under supervision of eSolutions staff. Devices must be stored in a secured (locked) location.	Backup devices must only be accessed in an emergency or failure of non-removable storage devices.	Information must only be stored on transportable and removable storage devices if they are secondary (backup) devices under the control of eSolutions. Contracts with 3rd party providers must include appropriate Standards for Data Protection and privacy clauses.[1]	Information must be encrypted using an approved encryption method during transmission and whilst stored on secondary devices.	Information must be removed before the secondary storage device is retired or reused. If the information cannot be removed, the device must be destroyed.

1[1] Contracts with 3rd party providers are negotiated by the Supply Chain Management Office, eSolutions working with the University Solicitor's Office.

Monash University Procedure

Protected	Access to records and files must be restricted to specific job roles, and requires authentication and password protection. Repairs to storage devices must be undertaken onsite and under supervision of Monash staff. Transportable devices must be stored in a secured (locked) location.	Use is prescribed by the Information Owner and is available within the Information Owner's domain and to specific University domains. Generally not available outside the University (exceptions are Government bodies, financial institutions).	All storage devices.2[2] Contracts with 3rd party providers must include appropriate Standards for Data Protection and privacy clauses.3[3]	Information must be encrypted using an approved encryption method if transmitted outside the Monash network. Information may be transmitted unencrypted within the Monash network.	Information must be removed before the storage device is retired or reused. If the information cannot be removed, the device must be destroyed.
Restricted	Access to records and files requires authentication and password protection. Transportable devices should be stored in a secured (locked) location.	Use is prescribed by the Information Owner.	All storage devices. Contracts with 3rd party providers must include appropriate Standards for Data Protection and privacy clauses.3	Information may be transmitted unencrypted inside and outside of the Monash network.	Information should be removed before the storage device is retired or re-used.

Technical advice on the Standards may be sought from the Risk and Security section of eSolutions by contacting the IT Service Desk.

Responsibility
Information Owners
Information Custodians
Information Users

Interpretation

Keyword	**Interpretation**

2[2] Includes all non-transportable storage devices and transportable devices such as floppy discs, removable hard drives, CDs, DVDs, USB flash drives and memory sticks, laptops, tablet computers, PDAs, mobile phones, other devices.

3[3] Contracts with 3rd party providers are negotiated by the Supply Chain Management Office, eSolutions working with the University Solicitor's Office.

Monash University Procedure

MUST	The item is mandatory. See also **'waivers against must and must not'** below.
MUST NOT	Non-use of the item is mandatory. See also **'waivers against must and must not'** below.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing an alternative course. See **'deviations from should and should not'** below.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course. See **'deviations from should and should not'** below.

Waivers against 'MUST' and **'MUST NOT'**: Where it is required to deviate from a **'MUST'** or **'MUST NOT'** statement in these procedures, written approval must be obtained from the Information Owner and maintained in the Information Register for the functional unit. The following details must be supplied:

a) the reasons for the deviation;
b) an assessment of the residial risk resulting from the deviation;
c) a date by which to review the decision; and
d) management's approval.

Deviations from **'SHOULD'** and **'SHOULD NOT'**: Where it is required to deviate from a **'SHOULD'** and **'SHOULD NOT'** statement, written approval must be obtained as for a waiver, and should be retained by the unit.

Responsibility
Information Owners
Information Custodians
Information Users

Responsibility for implementation	Information Owners Deputy Vice-Chancellors Vice Presidents Pro Vice-Chancellors and President, Monash South Africa Deans of Faculties
Status	Revised
Approval Body	**Name**: Vice-President (Administration) **Meeting**: n/a **Date**: 12-September-2012 **Agenda item**: n/a
Definitions	**Approved encryption method**: A method of making data unreadable except to those in possession of special knowledge, usually referred to as a key, that has been approved by the Manager, Security and Risk Section, eSolutions. **Approved removal program**: A program to securely erase data from electronic media that has been approved by the Manager, Security and Risk

Monash University Procedure

	Section, eSolutions. **Information Owner**: An individual with the responsibility for coordinating the implementation of this policy and its procedures for a functional area of the University. The Information Owners for administrative, research and education information are listed in the Information Classification Registers. **Information Custodian**: An authorised individual who collects, stores or transmits electronic information pertaining to the university's activities of research, education and administration. **Information User**: An authorised individual who accesses electronic information pertaining to the university's activities of research, education and administration. **Information Classification Register**: A catalogue of data sets, images, audio and video media and any other electronically stored information detailing the Information Owner, server name, data description and assigned Electronic Information Security Classification. **Data Sets**: Data related to a specific purpose or topic.
Legislation Mandating Compliance	**Australia:** Privacy and Data Protection Act 2014 No.60 (VIC) Health Records Act 2001 (Vic) - note Health Privacy Principles within Act (Section 19 and Schedule 1) Protected Disclosure Act 2012 No. 85 (VIC) Higher Education Support Act 2003 (Commonwealth) - note Part 5-4 Management of Information, and specifically section 179-10 Use of Personal Information Education Services for Overseas Students Act 2000 (Commonwealth) - specifically The National Code 2007, Standard 3.1(d) Public Records Act 1973 (Vic) Epidemiological Studies (Confidentiality) Act 1981 (Commonwealth) - where relevant to a research project **South Africa:** South African Electronic Communications and Transactions Act 2002 (Act No 25 of 2002) - protects personal information that has been obtained via an electronic medium. South African Protected Disclosures Act 2000 (Act No 26 of 2000)
Related Policies	Electronic Information Security Policy Recordkeeping: Retention and Disposal of University Records Policy Conduct and Compliance Procedure - Privacy Privacy of Student Records Policy
Related Documents	Monash Privacy Compliance Framework