Monash University Procedure

Procedure Title	Electronic Information Security – Information Classification Procedure
Parent Policy	Electronic Information Security Policy
Date Effective	01 August 2017
Review Date	01 August 2020
Procedure Owner	Chief Information Officer
Category	Operational – Information Technology
Version Number	2.0
Content Enquiries	IT Service Desk - http://monash.edu/esolutions/contact security@monash.edu
Scope	• All campuses in Australia • Monash South Africa • Monash College Pty Ltd • All staff, students and other Authorised Users
Purpose	Define the information classification framework, roles and responsibilities for information assets, the requirements for asset classification and risk assessments.
PROCEDURE STATEMENT	

1. Procedure Overview

What is Information Classification?

Information classification is the process of assigning level of classification to information assets that considers the impact as defined in the Monash risk framework, to ensure the level of information protection controls are commensurate with information value. Value as is also synonymous with the impact that would be experience should any of the following threats be realized in table 1.

Threat	Description	Risk domain
Disclosure	Unauthorized access to an asset	Confidentiality
Modification/ Fabrication	Unauthorized tampering or falsely fabrication of an asset	Integrity
Theft/loss	Theft or loss of information or other resources	Availability
Destruction	Destruction of information or resources	Availability
Interruption/ Denial of Service	Information, resource, or service becomes temporarily unavailable or unusable	Availability

Table 1 Threats

Why is information classification Important?

Information asset classification and labelling is important as communicates the value of the set by the owner to other parties as to how the information is to be handled in both physical and digital contexts, it also provide consistency for the application of security controls.

From an information systems architecture and design perspective the classification provides the designer the baseline minimum controls which need to be applied to the systems to ensure the asset protection is commensurate with its value.

Who is responsible in Monash?

The following roles / groups, are responsible for meeting the requirement contained in this procedure:

- Information Asset owners
- Information asset custodians

2. Procedure Requirements

Assess and Classify Information

Control Objective: to evaluate and an assign a classification level

PR/INC-010	Classify and label their assets in-accordance with Table 2 in this procedure.
PR/INC-020	Assign information asset custodians for the protection of their information assets
PR/INC-030	Register their assets with the classification attributes with the designated Monash Enterprise asset management systems with all relevant information system managers. *Note: this currently is managed by the records management team*
PR/INC-040	Authorise access to their information assets
PR/INC-050	Review who has access to their assets on a biannual basis for assets that classification rating of Protected (C), High (I), Class B(A), or higher for any one of those attributes.

3. Information Classification Framework

The tables, below outlines the rating descriptions for the security labels for Confidentiality, Integrity, and Availability (CIA). The rating drives the minimum security baseline controls as defined in the ***"Electronic Information Security Minimum Security Controls Procedure"***. Each asset must be label with rating that is commensurate with its risk profile.

Information asset classification

Monash University Procedure

To classify and information Asset the information asset owner must assume that no security controls have been applied, and determine what the impact to the organisation would be in a worst case scenario should there be a breach of Confidentiality, Integrity or Availability.

Note: When designing information systems that aggregate information assets the rating needs to be based on the loss/disclosure/modification of those assets. Eg losing one student records is likely to have a low impact, whereas the loss of an entire student database, is likely to have a catastrophic impact.

When Assets of different classifications are stored in a combined into a single, logical entity, the principle of highest classification shall apply and controls shall be implemented accordingly.

Confidentiality Classification Labels

Table 2, below describes the organizational impact and the confidentiality **label** in bold.

Security Objective	Impact	Information Classification Criteria and labelling
Confidentiality	Catastrophic (A)	Information that may result in a Catastrophic or Major impact from disclosure event is classified as **Critical (C = 4)**.
	Major (Ma)	
	Moderate (Mo)	Information that may result in a Moderate impact from disclosure event, is classified as **Protected (C = 3)**
	Minor (Mi)	Information that may result in a Minor impact from disclosure event, is classified as **Restricted (C = 2)**
	Insignificant (I)	Information that may result in an Insignificant impact from disclosure event, is classified as **Public (C = 1)**

Table 2

Monash University Procedure

Integrity Classification Labels

Table 3, below describes the organizational impact and the integrity **label** in bold.

Security Objective	Impact	Information Classification Criteria
Integrity	Catastrophic (A)	Information that may result in a Catastrophic or Major impact from a modification/fabrication/corruption event, is classified as **Absolute (I = 4)** **Absolute** requirement implies that no inaccuracies or omissions can be tolerated.
	Major (Ma)	
	Moderate (Mo)	Information that may result in a Moderate impact from a modification/fabrication/corruption event, is classified as **High (I = 3)** **High** requirement, meaning that a loss of integrity would cause significant embarrassment and disruption and might be difficult to detect.
	Minor (Mi)	Information that may result in a Minor impact from a modification/fabrication/corruption event, is classified as **Moderate (I = 2)** **Moderate** requirement, meaning that the organisation would be somewhat affected by a loss of integrity, but the situation could be easily detected and recovered.
	Insignificant (I)	Information that may result in an Insignificant impact from a modification/fabrication/corruption event, is classified as **Low (I = 1)** **Low** requirement, such that there would be minimal impact if the data were inaccurate or incomplete.

Table 3

Monash University Procedure

Availability Classification Labels

Table 4, below describes the organizational impact and the Availability **label** in bold.

Security Objective	Impact	Information Classification Criteria
Availability	Catastrophic (A)	Information that may result in a Catastrophic or Major impact from a data destruction/loss/interruption/DoS event, is classified as **Class A (A = 4)** **Class A** is consider a Mission Critical service.
	Major (Ma)	
	Moderate (Mo)	Information that may result in a Moderate impact from a data destruction/loss/interruption/DoS event, is classified as **Class B (A = 3)** **Class B** Business Essential service.
	Minor (Mi)	Information that may result in an insignificant impact from a data destruction/loss/interruption/DoS event, is classified as **Class C (A <= 2)** **Class** Business Supporting service Business Supporting service
	Insignificant (I)	

Table 4

4. Responsibilities for Information Assets and Information Risk Management.

Information Asset Owners

4.1 Delegate to an approved custodian the protection of their information assets.

4.2 Ensure their information assets are classified.

4.3 Approval of physical and logical access requests.

4.4 Review of users' access rights at regular intervals.

Chief Information Officer (Information asset custodian)

4.5 The custodian shall typically, but not necessarily be confined to maintain an information asset inventory (CMDB).

4.6 Assist the information asset owner in the identification of control mechanisms, ensuring their development, implementation, maintenance and effective operation.

4.7 Reporting issues that affect the information asset in the operational environment to the asset owner.

Third Parties

4.8 Third parties shall comply with Monash University information security policies, procedures and ICT Security Framework.

End Users

4.9 Users shall be responsible and accountable for; activities associated with an assigned account; protecting the secrecy of confidential information; reporting known or suspected security incidents; and complying with Monash University Information Technology acceptable use policies.

Security Classification Definitions

4.10. Information based on its confidentiality shall be classified as one of the following:

Critical, this classification applies to highly sensitive information where:

- Access, distribution, retention and/or destruction of information is subject to restrictive regulatory obligations;
- Unauthorized disclosure would seriously and adversely impact the University, its employees, its students and/or its partner organizations;
- Access is strictly limited to a selected group or process; and
- If compromised, would place the University in breach of its legal and regulatory responsibilities.

Protected, this classification applies to sensitive information where**:**

- Unauthorized disclosure may adversely impact on the University, its employees, its students and/or its partner organizations; and
- Access is limited to a selected group or process.

Restricted, this classification applies to confidential information where:

- Does not include sensitive information, but is created or received within the University (including by students) and used internally;
- Disclose would not cause damage to the University, its employees, its students and/or its partner organizations;

Public, this classification applies to publicly available information where:

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

Examples of information according to their confidentiality classification

The following are examples of data for each data classification. These examples are not extensive and should be used only as a guideline.

Classification	Examples
Critical	• Credit card numbers. • Tax file numbers. • Reportable Police Information (incidents and violations). • Information classified by Human and Animal Ethics Committees. • Any personal identifiable information combined with health or sensitive information. • Information that could be associated to an individual's racial or ethnic origin, religious beliefs, sexual orientation, etc. For more information, please see the definition of sensitive information. • Information subject to regulatory compliance.

Monash University Procedure

Classification	Examples
Protected	• Financial information, such as purchase orders not subject to regulatory compliance. • Discipline Committee Meeting Minutes. • Staff Employment Contracts. • Student Evaluation of Teaching and Units data. • Research data set inputs where data is not combined with personal identifiable information. • Communications with research partners. • Personal identifiable information.
Restricted	• Course materials and content. • Marketing strategy and materials. • Educational resources. • Monash only training.
Public	• The Monash University home page (www.monash.edu.au). • Faculty course lists and the University Handbook. • Monash research achievements and broadcast events.

Responsibility for implementation	Chief Information Officer Information Owners Deputy Vice-Chancellors Vice Presidents Pro Vice-Chancellors and President, Monash South Africa, Monash Malaysia Deans of Faculties
Status	Revised
Approval Body	**Name:** Chief Information Officer **Meeting:** N/A **Date:** 01 – August - 2017 **Agenda item:** N/A **Author:** Cesar Guzman – IT Security and Risk Consultant.
Definitions	**Risk Assessment:** the determination of quantitative or qualitative estimate of risk related to a well-defined situation and a recognized threat. **Information Asset:** a body of knowledge that is organized and managed as a single entity. Like any other corporate asset, an organization's information assets have financial value. **Information Asset Owner:** responsible for ensuring that specific information

	assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited. **Personal Identifiable Information:** is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. **Information asset custodian:** person responsible for the safe custody, transport, storage of the data and implementation of business rules. **Information security attributes:** Confidentiality, integrity and availability is a model designed to guide policies for information security within an organization. **Confidentiality:** is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes **Integrity:** involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that unauthorized people cannot alter data. **Availability:** refers to ensuring that authorized parties are able to access the information when needed. Information only has value if the right people can access it at the right times
Legislation Mandating Compliance	**Australia** Information Privacy Act 2000 (Vic)- note Information Privacy Principles within the Act (Section 14 and Schedule 1) Privacy Act 1988 (Commonwealth) Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth) Health Records Act 2001 (Vic)- note Health Privacy Principles within Act (Section 19 and Schedule 1) 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) Epidemiological Studies (Confidentiality) Act 1981 (Commonwealth) - where relevant to a research project (needed) Public records Act 1973 (VIC) Monash University (Council) Regulations Part 7 Monash University (Vice-Chancellor) Regulations Part 5 Monash University Statute **South Africa** 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.

Monash University Procedure

	South African Protected Disclosures Act 2000 (Act No 26 of 2000)
Related Policies	Information Technology Acceptable Use Policy. Risk Management Policy.
Related Documents	IT Risk Management Manual Risk Management Procedures