Monash University Policy

Policy Title	Electronic Information Security Policy
Date Effective	01 June 2017
Review Date	(*Under review*)
Policy Owner	Chief Information Officer
Category	Operational
Version Number	2.2 (*Administrative amendments effective 02 April 2021*)
Content Enquiries	security@monash.edu
Scope	For the purposes of this policy, references to 'the University' includes all users at Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College Pty Ltd, Monash Suzhou and the Monash University Prato Centre, unless otherwise indicated.
Purpose	To define the information classification framework; management; roles and responsibilities for information assets and the controls that apply to each classification. To apply proportionate and effective management of information security risks throughout Monash University, enable the conduct of the University's business and provide directives for the protection of the University's information assets. To authorise the establishment of the Information Security Management System (ISMS).

POLICY STATEMENT

1. Information and information asset classification.

1.1. University information assets shall be managed according to its value and importance to the achievement of the University's strategic goals.

1.2. Information assets must be classified according to the impact that Monash would incur in case of an incident affecting any, or all, security attributes of the asset.

1.3. Risk assessments shall be performed where required, following mechanisms as defined in the IT Risk Management Manual.

2. Information security roles and responsibilities.

2.1. Roles and responsibilities shall be defined for the ownership and protection of information assets.

2.2. The Chief Information Security Officer is responsible for the development and maintenance of the University's Information Security Management System (ISMS).

2.3. The IT Security and Risk Steering Committee will maintain oversight of the University's IT risk profile.

3. Breaches of this Policy and its Procedures

3.1. The University treats any breach of its policies, procedures and schedules seriously; it encourages reporting of concerns about non-compliance, and manages compliance in accordance with the applicable Enterprise Agreement, relevant instrument of appointment and/or applicable contract terms. A failure to comply may result in action by the University. Such action may include disciplinary and other action up to and including potential termination of employment for employees, or the cessation of engagements with the University for other persons.

3.2. Breaches of this Policy and its procedures may also result in suspension of access to University IT resources.

3.3. Other users not related to Monash University may be subject to appropriate action as determined by the University..

3.4. Breaches of this policy and its procedures may also be reported to external parties as required under law.

Supporting Procedures	Electronic Information Security: Callista Access Procedures Electronic Information Security: Payment Card Industry Data Security Standard (PCI DSS) Procedures (Australia only) Electronic Information Security: Information Classification Procedure
Responsibility for implementation	Chief Information Officer CEO, Monash College PVC Monash University Indonesia PVC Monash University Malaysia
Status	Revised
Approval Body	**Name:** Chief Information Officer **Meeting:** N/A **Date:** 01 – August - 2017 **Agenda item:** N/A
Endorsement Body	**Name:** Chief Information Officer **Meeting:** N/A **Date:** 01 – August - 2017 **Agenda item:** N/A
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 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 2014 (Vic): note Information Privacy Principles within the Act (Section 14 and Schedule 1) 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) – The National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code 2018) 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. South African Protected Disclosures Act 2000 (Act No 26 of 2000) **Malaysia** Personal Data Protection Act 2010 Private Healthcare Facilities & Services Act 1998 The Private Higher Educational Institutions Act, 1996 (amended 2009) The Universities and University Colleges (Amendment) Act, 1996 (amended 2009)
Related Policies	Information Technology Acceptable Use Policy
Related Documents	N/A