MONASH University

INFORMATION SECURITY AND CLASSIFICATION MANAGEMENT PROCEDURE

SCOPE

This procedure applies to all Monash University staff and associates responsible for the access, management and use of the University IT environment.

For the purposes of this policy, references to 'the University' include Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College, Monash Suzhou, the Monash Prato Centre, and the World Mosquito Program Ltd (and its subsidiaries).

PROCEDURE STATEMENT

This procedure defines the information security classification framework, roles and responsibilities for information assets, the requirements for asset classification, and risk assessments.

For the purpose of this policy, 'information assets' refers to digital assets encompassing any form of information, data or content that is held in online systems, network and storage.

1. Information Classification

1.1 Information assets will be assigned a level of classification to ensure the information protection controls are commensurate with the information value as outlined in Table 1.

Table 1: Threat domains to information assets

Threat	Description	Risk domain
Disclosure	Unauthorised access to an asset	Confidentiality
Modification/Fabrication	Unauthorised tampering or false 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

1.2 When classifying an information asset, the owner must assume that no security controls have been applied and determine the impact to the University were the asset to have a breach of confidentiality, integrity or availability.

1.3 The classification labels in regard to confidentiality, integrity and availability are listed in Tables 2, 3 and 4 below:

Table 2: Confidentiality classification of informations assets

Security Objective	Impact	Information Classification and Labelling
Confidentiality	Catastrophic (A)	Information that may result in a Catastrophic or Major impact from disclosure is classified as **Very Sensitive. (C = 4)**
	Major (Ma)	

Security Objective	Impact	Information Classification and Labelling
	Moderate (Mo)	Information that may result in a Moderate impact from disclosure is classified as **Sensitive. (C = 3)**
	Minor (Mi)	Information that may result in a Minor impact from disclosure is classified as **Restricted. (C = 2)**
	Insignificant (I)	Information that may result in an Insignificant impact from disclosure is classified as **Public. (C = 1)**

Table 3: Integrity classification of information assets

Security Objective	Impact	Information Classification and Labelling
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 reputational damage and disruption.
	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.
	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 4: Availability classification of information assets

Security Objective	Impact	Information Classification and Labelling
Availability	Catastrophic (A)	Information that may result in a Catastrophic or Major impact from data destruction/loss/interruption is classified as **Class A. (A = 4)** **Class A** is considered a mission critical service
	Major (Ma)	
	Moderate (Mo)	Information that may result in a Moderate impact from data destruction/loss/interruption is classified as **Class B. (A = 3)** **Class B** is considered a business essential service
	Minor (Mi)	Information that may result in a Minor or Insignificant impact from data destruction/loss/interruption is classified as **Class C. (A <= 2)** **Class C** is considered a business supporting service
	Insignificant (I)	

2. Information Applications and Systems

2.1 Information systems must be assigned a weighting based on the aggregate information assets stored in the system and likelihood of impact of partial compared to full system breaches. For example, the impact of losing one student record is likely to have a minor impact, whereas the loss of the entire student database is likely to have a catastrophic impact.

2.2 Information assets stored across multiple systems will be assigned the highest level of classification based on the highest classified information asset and any controls based on the highest classified asset must be implemented accordingly.

2.3 Any systems that store or process University information/data must meet the technical controls outlined in the Cyber Security Management Policy and staff are required to complete a Privacy Impact Assessment and an Information Security Risk Assessment (ISRA) prior to the system being implemented or a change to the system is made that may impact on the storage or processing of information.

2.4 Changes to applications or systems must be made in accordance with the change control processes and established secure software development lifecycle (SDLC) control standards, and any additional processes required by eSolutions.

2.5 Any copies of production data must only be stored in agreed secure environments. Data used for development environments must be scrambled or masked to ensure the data is desensitised.

2.6 Source codes must be kept secure and version controlled to maintain the integrity, confidentiality and copyright, and the applicable coding standards must be followed.

2.7 When implementing a change to existing systems or changes to the type of information asset stored or utilised by the system, any potential security issues must be documented and reported to the Cyber Risk and Resilience team by submitting an Information Security Risk Assessment (ISRA).

2.8 Any data integrations between systems must be designed and implemented following the relevant security standards.

2.9 Enterprise system classifications are listed on the Cyber Risk and Resilience intranet page.

3. Asset Owners and Users

3.1 Information asset owners must ensure the asset is classified, delegate an approved custodian (if applicable) the responsibility for protection of the asset, and approve, monitor and review user access rights. A review of user access rights should be conducted annually at a minimum.

3.2 User access rights must be set to the lowest level of information access required for a user to perform their role.

3.3 Any suspicious activity, potential or actual cyber security incidents must be reported to eSolutions via the website or via email to cyberteam@monash.edu as soon as practicable. This includes incidents of an accidental nature, such as a lost laptop or device. If an incident involves personal information, it must also be reported to the University's Data Protection and Privacy Office.

DEFINITIONS

Availability	Ensuring that authorised parties are able to access the information when needed.
Confidentiality	Ensuring that information is not made available or disclosed to unauthorised individuals, entities, or processes
Business critical	A task, service or system whose failure or disruption would impact the ongoing or ultimate success of a business, but do not cause immediate impact to operations.
Information Asset	A body of knowledge that is organised and managed as a single entity, such as a database of contacts, or University research data. Like any other corporate asset, the loss of the University's information assets has a financial impact
Information value	The value ascribed to an information asset consistent with the financial and reputational impact that would be felt should any threats be realised.
IT environments	For the purpose of this policy, 'IT environments' includes all IT infrastructure including hardware, software, networks, systems and services owned or controlled by the University, or any University controlled or associated entity.
Integrity	The maintaining of consistency, accuracy, and trustworthiness of data over its entire life cycle. Data shall not be changed in transit, and steps shall be taken to ensure that unauthorised people cannot alter data
Mission critical	A task, service or system whose failure or disruption would cause an entire operation or business to grind to a halt. It is a type of task, service, or system that is indispensable to continuing operations.

GOVERNANCE

Parent policy	Cyber Security Management Policy
Supporting procedures	
Supporting schedules	N/A
Associated procedures	
Related legislation	N/A
Category	Governance
Approval	Chief Operating Officer & Senior Vice-President 28 February 2023
Endorsement	Chief Digital and Student Services Officer 28 February 2023
Procedure owner	Chief Information Security Officer
Date effective	6 April 2023
Review date	6 April 2026
Version	3.0
Content enquiries	cyberteam@monash.edu