MONASH University

INFORMATION CLASSIFICATION AND HANDLING STANDARD

Introduction **2**
- Purpose 2
- In Scope 2
- Out of Scope 2
- Attributes 3
- Security Architecture Principles 3

Security Standards for Information Classification **4**

Security Standards for Information Handling **7**

Reference **16**

Definitions **16**

Version and Update History **18**

Introduction

Purpose

The purpose of this document is to guide project and operational teams in the classification and handling of information assets within the organisation. Information assets refers to any data, information, or intelligence classified and/or handled by an organisation. It outlines the Monash University Cyber Risk and Resilience team's requirements and recommendations in order to make sure cyber security risks are mitigated to the university's acceptable level. This helps to ensure appropriate protections for the vast range of information assets within the university, and to assist with legislative and regulatory requirements.

This standard is developed in line with the existing University's cyber security standards and does not supersede them. Please refer to the cyber security standards for specific security requirements (e.g. approved encryption algorithms). In addition, please refer to the Approved Services and Classification Levels document for specifics.

Please engage the Cybersecurity Architecture or Group Information and Records Management for any clarification and if certain service categories or design considerations are not covered by this baseline.

This standard includes:

- Information Classification
- Information Handling

In Scope

This standard applies to all Monash University staff, students, associates and visitors accessing and using the University's Information Technology (IT) environments. For the purpose of this standard, references to 'the University' include the activities of Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College, Monash Suzhou, Monash University Prato Centre and the World Mosquito Program Ltd (and its subsidiaries), unless otherwise indicated. In the scope of this document:

- Information assets, both internally and externally stored or handled
- Virtual or physical systems supporting or storing this information

Out of Scope

Out of the scope of this document:

- Relevant management and operation models

- Security training and awareness requirements
- Step by step implementation guides

Attributes

Attributes Supported: Protected, Secure, Trusted, Auditable, Isolated, Identified, Resilient, Zoned

Security Architecture Principles

Cyber Security Architecture Principles should be considered in order to protect Monash University's environment.

Security Standards for Information Classification

This section covers the minimum security controls for information classification.

Table 1. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Identify	Information Asset Protection	• Classify information in accordance with the Monash University Information Security and Classification Management Procedure as outlined in table 2 below.

The following table is a summary of the Monash University Information Confidentiality Classification Levels.

Table 2. Classification Levels		
Classification Level	**Description**	**Examples**
Public	• It is made available, or released to the general public; • No adverse effects are expected to result from the wide circulation of this information.	**Institutional** • The Monash University home page (www.monash.edu) and web presence. • Faculty course lists and the University Handbook. • Monash research achievements and Public broadcast events. • Information in the public domain. (e.g. Information intentionally made public. i.e, does not include breached/compromised data available in public)

		• General institutional and business information that can be made public **Research** • Monash research achievements and public broadcast events. • Publicly released annual reports (e.g. clinical study reports). • Published research data/information in Bridges or discipline repositories.
Restricted	• Unauthorised access, modification, distribution, retention and/or destruction or disclosure may have a negligible impact on the University, its employees, its students and/or its partner organisations; • Does not include very sensitive or sensitive information, but is created or received within the University (including by students) and used internally; • Disclosure would not cause damage to the University, its employees, its students and/or its partner organisations.	**Institutional** • Course materials and content. • Educational resources. • Training material. • Building plans and associated information. • Internal processes and procedures. **Research** • **De-identified data** that is aggregate data with no identifying information included e.g. counts of patient admissions to ICU ward per month. • Drafts of research publications that do not contain identifiers • Data from instruments and imaging systems (excluding those linked to an MRN or patient ID) that do not contain identifiers

		• Data from sensors, cameras, recorders etc. that do not contain identifiers (e.g. faces) any any sensitive or very sensitive data
Sensitive	• Unauthorised access or disclosure may adversely impact on the University, its employees, its students and/or its partner organisations; • Access, modification, distribution, retention and/or destruction is limited to a selected group or process; and; • If compromised, may place the University in breach of its legal and regulatory responsibilities.	**Institutional** • Financial information excluding very sensitive information • Student information e.g. exam results and material. • Staff information e.g. details of employment. • Student evaluation of teaching and units data. • Personal contact information e.g. name, email, phone number, address. • Infrastructure and network Diagrams • Login details, eg, credentials, secret keys, API keys **Research** • **Re-identifiable data** where direct identifiers have been removed but other indirect identifiers may be present e.g. Postcode + rare ICD-10 code still present. • Research datasets where data is not combined with personal identifiable information. • Communications with research partners.
Very Sensitive	• Unauthorised access or disclosure would seriously and adversely impact the University, its employees, its students and/or its partner organisations; • Access, modification, distribution, retention and/or destruction of information is subject to restrictive regulatory obligations;	**Institutional** • Payment Card Information. • Tax File Numbers. passport, drivers licence, Medicare details, Centrelink details, Government issued identity card information, social security number etc. • Any personally identifiable information combined with health, biometric data or sensitive information.

	● 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.	● Information that could be associated with an individual's racial or ethnic origin, religious beliefs, sexual orientation, etc. ● Police verification data check **Research** ● **Identifiable data** containing multiple direct identifiers e.g. Name, MRN, DOB and contact details. ● Information classified by Human and Animal Ethics Committees. ● Any information on children or young persons.

Security Standards for Information Handling

Classification Level	Control Type	Security Control
Public	**Data Access**	• All access to information is logged.
	Information Governance	• The roles and responsibilities of Information Governors, Information Stewards and Information Administrators are defined according to the University's Information Management Policy, Information Governance and Recordkeeping Procedure and Information Management Framework. • Record, maintain and classify information assets based on their sensitivity.
	Data Transmission	• Users transferring data to and from systems are held accountable for data transfers they perform.
	Data Storage	• Classify network drives and file shares based on the sensitivity classification of the data it stores. • Media is sanitised before it is used for the first time.
	Data Classification	• Classify data in accordance with Monash University Classification Procedure. Refer to Security Standards for Information Classification above. • Use the university approved data marking tool where possible.
	Data Retention	• Decisions to retain records are made in accordance with the Monash Retention and Disposal Authority.
	Data Destruction	• Decisions to dispose of records are made in accordance with the Monash Retention and Disposal Authority.

Restricted *Plus all controls listed in Public categories*	**Data Access**	• Review and update access agreements yearly in line with the Information Technology Acceptable Use Procedure. • Enforce approved authorisations for logical access to information and system resources in accordance with applicable access control policies.
	Information Governance	• Ensure risk management policy and procedures are in place and being complied with. Upon a related change, align with the University Change Management System and consult with this standard and any related baselines. Should the change use cases not be covered, commence a risk assessment as per the University risk management system.
	Data Transmission	• Only authorised file sharing services are used and undertaken inline with the approved services list for varying levels of sensitivity. • Very Sensitive, Sensitive, and Restricted information are not sent to personal email addresses and non-enterprise cloud storage. Relevant process and technology controls are implemented to achieve this. • When printing documents containing Very Sensitive, Sensitive and Restricted information, use the University enterprise print management solution. • When manually importing data to systems, the data is scanned for malicious and active content. If data fails security checks it is quarantined until reviewed and either approved or not approved for release. • When manually exporting data from systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release. • Data and information involved is encrypted whilst in transit, in line with the University cryptography guidelines.
	Data Storage	• Where data is stored in the cloud environment, mandatory controls are enforced in line with the University Cloud Security Standard.

		• Removable media devices are blocked unless they have been approved for use. See Asset Management Standard. • If Very Sensitive, Sensitive or Restricted documents are printed, one is to remain by the printer until all documents are printed. Documents are not left unattended at the printer. • Where applicable, a removable media register is developed, implemented, maintained and verified on a regular basis. • Media is classified to the highest sensitivity or classification of data it stores, unless the media has been classified to a higher sensitivity or classification. • Data is encrypted at rest in line with the University cryptography guidelines.
	Data Classification	• Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments. • Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate. • Protective marking tools do not automatically insert protective markings into emails. • Protective marking tools do not allow users replying to or forwarding emails to select protective markings lower than previously used. • Media, with the exception of internally mounted fixed media within ICT equipment, is labelled with protective markings reflecting its sensitivity or classification. • When manually exporting data from systems, the data is checked for unsuitable protective markings. • Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
	Data Retention	• Data that is to be kept permanently are archived according to the Information Management Policy and Retention and Disposal Authority. • Research data are retained in accordance with the Research Data Management Policy.

		• Retention of data should be in accordance with the Monash Retention and Disposal Authority.
	Data Destruction	• Disposal of information should be in line with the Monash Retention and Disposal Authority. • Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use are removed prior to its disposal.

Sensitive
Plus all controls listed in Public and Restricted categories
	Data Access	• Implement monitoring and alerting for unauthorised user and application access to Sensitive and Very Sensitive information.
		• Conduct quarterly access audits for systems with Sensitive information.
		• Only approved users are allowed to access Sensitive and Very Sensitive data.
		• Identify and document user access roles based on their specific support or business function, following the separation of duty principles.
		• Define system access authorisations to support separation of duties.
		• Implement the principle of least-privilege and need-to-know when granting access to systems holding sensitive data.
		• Restrict access to systems holding sensitive data to Information Governors, Information Stewards and Administrator as required by role and approved by the Information Governors.
		• Very Sensitive and Sensitive documents are stored in secure cabinets within a secure access area.
		• Enforce the University's approved Multi-Factor Authentication (MFA) solution for systems and services hosting Very Sensitive and Sensitive data.
		• Verify that individuals requiring access to organisational information and systems:
		  ○ Sign appropriate access agreements prior to being granted access; and
		  ○ Enforce expiry date on access and require re-signing once expired.
		  ○ If access agreements are updated, users are required to sign the updated agreement.

	Information Governance	• For systems and services supporting and/or storing Sensitive information, third party assurance actions are required, e.g. Vendor Risk Assessment.
		• Applicable legal and regulatory requirements are formally identified based on the information classification.
		• Maintain compliance to legal and regulatory requirements.
		• Contracts outlining any requirements for accessing the University's information and/or services are required prior to providing access to third parties.
		• Reference asset management policy and procedures are in place and being complied with.
		• Record and maintain an inventory of systems and software used to manage the data in the system.
		• Assets used to support, store and handle Very Sensitive and Sensitive data are recorded and maintained in line with the Asset Management Standard. At a minimum, the following details are captured:
		  ○ IP address
		  ○ Hostname
		  ○ Location
		  ○ Software installed
		  ○ Purpose of server or service
		  ○ Integrations
		  ○ Person responsible
		  ○ Team responsible
		  ○ Information classification level of the system

	Data Transmission	• Only approved and authorised devices and removable media are used to export Sensitive and/or Very Sensitive information. • Data exported from Sensitive and Very Sensitive systems is reviewed and authorised by a responsible role such as the Data Governor or delegate beforehand.

		• Data authorised for export from Sensitive and Very Sensitive systems is digitally signed by a trusted source. • Data transfer logs are used to record all data imports and exports from systems. • Data transfer logs for Sensitive systems are fully verified at least quarterly. • Data in outgoing emails is monitored and/or prevented against a set of Data Loss Prevention (DLP) defined rules using a DLP tool or email gateway.
	Data Storage	• Media is only used with systems that are authorised to process, store or communicate its sensitivity or classification. • Media containing Sensitive and Very Sensitive Information are backed up as per the relevant section in the University's cyber security standards, policies and with reference to any relevant regulatory requirements. • Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured. • Before reclassifying media to a lower sensitivity or classification, the media is sanitised or destroyed, and a formal administrative decision is made to reclassify it. • Following sanitisation, Very Sensitive and Sensitive non-volatile media retains its classification. • Monitor for file transfers to physical media storage and review logs quarterly. • Sensitive data that may be held within logs and tracked events are sanitised and/or anonymised. These logs should only be sent to trusted services such as the enterprise approved solution. • Where data has to be hosted or stored offshore, a thorough security review and approval by the Cyber Risk and Resilience team is required. • Where data has to be hosted or stored offshore, applicable compliance, legal and regulatory requirements of the offshore hosting location are followed.

		• Hardened workstations and servers are used when storing or handling Very Sensitive and Sensitive information. • Backups are encrypted in line with the University's cryptography guidelines. • Backup and restore effectiveness are regularly tested with reference to the University's backup and restore policy.
	Data Classification	• Use traceable data classification tags to facilitate the implementation of asset protection solutions, including the use of barcodes for physical assets.
	Data Retention	*Refer to the Data Retention controls in Public and Restricted categories.*
	Data Destruction	• Disposal of information should be in line with the Monash Retention and Disposal Authority. • Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use are removed prior to its disposal. • Data destroyed by third party vendors are verified by the Information Steward or Data Administrator to confirm destruction. • Faulty or damaged media that cannot be successfully sanitised is destroyed prior to its disposal. • Where required, following sanitisation, destruction or declassification, a formal administrative decision is made to release media, or its waste, into the public domain.
Very Sensitive *Plus all controls listed in Public, Restricted and Sensitive categories*	**Data Access**	• Conduct monthly access audits for systems with Very Sensitive information. • Where access to Very Sensitive data is required by a third-party, a thorough security review and approval by the Chief Security Information Officer (CISO) is required. • Enforce Just-in-Time (JIT) access to systems hosting Very Sensitive data.
	Information Governance	• A comprehensive risk register on the handling of Very Sensitive data is developed, implemented, maintained, and reviewed on a regular basis.

		• All users are required to complete the University's mandatory cyber security awareness training prior to handling Very Sensitive data, as per the University's Cyber Security Management Policy. • Users collecting, handling and managing Very Sensitive data should complete a request for an Information and Data Management Assessment for targeted review and guidance on information governance, collection, management and disposal of information.
	Data Transmission	• Data transfer logs for Very Sensitive systems are fully verified at least monthly. • Trusted sources for Very Sensitive systems are limited to people and services that have been authorised as such by the Cyber Risk and Resilience team. • When manually exporting data from Very Sensitive systems, digital signatures are validated and keyword checks are performed within all textual data. • Where Very Sensitive data are transmitted via the internet or a public endpoint, a thorough review and approval by the Cyber Risk and Resilience team is required. • Where Very Sensitive data is leaving the University's environment, it is monitored against a set of DLP defined rules from a DLP tool or solution. • Monitor for file transfers to physical media storage and review logs monthly. • Consider enforcing application layer encryption to Very Sensitive data passing through the application before storing it in the database.
	Data Storage	• Where Very Sensitive data has to be stored outside the University's on-premises environments, a thorough security review and approval by the Cyber Risk and Resilience team is required. • Perform the required third party assurance actions when new services, solutions or components outside the approved services list are required to host or store Very Sensitive data.
	Data Classification	*Refer to the Data Marking controls in Public, Restricted and Sensitive categories.*

	Data Retention	*Refer to the Data Retention controls in Public, Restricted and Sensitive categories.*
	Data Destruction	*Refer to the Data Destruction controls in Public, Restricted and Sensitive categories.*

Reference

Monash University Cyber Security Management Policy

Monash University Cyber Security Architecture Principles

Monash University Cyber Security Standard

Monash University Asset Management Standard

Monash University Information Management Policy

Monash University Information Governance and Recordkeeping Procedure

Monash University Information Management Framework

Definitions

Table 4: Definitions	
Term	**Definition**
CISO	Chief Security Information Officer.
Information owner	The owner of any form of intellectual property.
Information Governor	Usually a Director for their area, this role is accountable for ensuring that the data asset under their governance is compliant with university data policies and standards.
Information Steward	Also a senior business role, this role is responsible for the quality and integrity of the data in the data asset.
Information Administrator	Usually a system-focused SME or IT professional, this role is responsible for managing the actual data asset, protecting data and preventing unauthorised use.
Information asset	A collection of data that has inherent or recognised value to an organisation.
Just-in-Time	The privilege granted to access applications or systems is limited to predetermined periods of time, on an as-needed basis.
Non-volatile media	Physical media that retains data without electrical power. This means that data is permanently stored and it is not lost when power to the device is turned off.
Data sanitisation	Purposely, permanently erasing or destroying data from a storage device, to ensure it cannot be recovered.
Protective markings	Security labels that act as a visual indication to those who are handling the information. The markings convey the minimum level of confidentiality and security required when handling the information.
Application Layer Encryption	A data-security solution that encrypts any type of data passing through an application. When encryption occurs at this level, data is encrypted across multiple (including disk, file, and database) layers.

Version and Update History

Version	Date	Author/Reviewer	Role	Team	Summary of Change
0.1 Draft	03/12/21	Ashley Niklaus	Enterprise Security Architect	Cyber Risk and Resilience	Initial Draft
0.2 Draft	06/12/21	Stanley Wijoyo, Simsam Hijjawi	Senior Enterprise Security Architect	Cyber Risk and Resilience	Internal Review
0.3 Draft	07/12/21	Ed Messina	Assistant Chief Information Security Officer	Cyber Risk and Resilience	Peer Review
1.0	09/12/21	Dan Maslin	Chief Information Security Officer	Cyber Risk and Resilience	Initial Release
1.1 Draft	09/08/23	Kate Matchett	Business Analyst	Cyber Risk and Resilience	Updates for version 2.0
1.2 Draft	18/08/23	Stanley Wijoyo	Senior Enterprise Security Architect	Cyber Risk and Resilience	Internal Review
1.2 Draft	18/08/23	Simsam Hijjawi	Cyber Security Architecture Manager	Cyber Risk and Resilience	Internal Review
1.3 Draft	06/09/23	Richard Sengmany	Cyber Risk Management Lead	Cyber Risk and Resilience	Peer Review
1.4 Draft	09/10/23	Fiona Neilson	Business Change Lead	Data Engineering Services	Peer Review
1.5 Draft	07/11/23	Ed Messina	Assistant Chief Information Security Officer	Cyber Risk and Resilience	Peer Review
2.0	21/11/23	Dan Maslin	Group Chief Information Security Officer	Cyber Risk and Resilience	Version 2.0 Release
2.1	17/06/24	Abi Vijay	Enterprise Security Architect	Cyber Risk and Resilience	Version 2.1 updates
3.0	11/07/25	Ashok Khatiwada Ed Messina Siddant Dan Maslin	Sec Arch Manager Interim CISO Director - Info &Records Group CISO	Cyber Risk and Resilience Info and Records Management	Some terminology changes and Info and Records Management now “Responsible”