CYBER SECURITY MANAGEMENT POLICY

SCOPE

This policy applies to all Monash University staff, students, associates, visitors and any user of the University's IT environments irrespective of location or device ownership, such as users with personally owned computers.

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).

PURPOSE

This policy establishes the University's and users' cyber security risk management responsibilities, which are based on the principle that cyber security is every user's responsibility.

For the purpose of this policy, 'information assets' refers to digital assets encompassing any form of information, data or content that is held in University IT environments.

POLICY STATEMENT

1. Principles

1.1 Effective management of cyber security helps protect the University from cyber threats that try to take advantage of opportunities in technology, people and processes to harm or misuse systems and assets owned or managed by the University.

1.2 The University manages cyber security risk to safeguard and secure the confidentiality, integrity and availability of its technology, applications and information assets, and facilitate a culture of cyber security awareness.

1.3 The management and awareness of cyber security risk is the responsibility of both the University and users, and requires a concerted effort across all University operations.

1.3.1 Monash University controlled entities that manage their own IT services and environments must be aware of their responsibilities under this policy, and as set out in clause 5.6.

1.4 The University's cyber security strategy and risk management responsibilities support the Group Risk Management and Compliance Policy and utilise risk-based decision making to manage cyber security risks. Cyber security controls are designed to:

- support the University's education, research and engagement activities;
- facilitate individual users' cyber security awareness to enable accountability and trust;
- be proportionate to the value of the system, application and information asset;
- support compliance with the University's legal obligations, including in relation to data protection and privacy and security of critical infrastructure;
- uphold confidentiality, integrity and availability of information assets; and
- allow for proactive plans and actions to detect, prevent and respond to cyber security threats.

2. Key Requirements

Cyber Security Framework

2.1 The University's cyber security framework establishes rules and functions to maintain an appropriate level of cyber security to protect its IT environments.

2.2 The cyber security framework is supported by the following four pillars;

- **Cyber security strategy:** provides an effective, adaptable and risk-based approach to the management of cyber risks to support the University in its mission.
- **Cyber security management:** ensures the management of cyber risk and resilience of technology across the University's global footprint.
- **Cyber security controls:** implement a multilayered cyber security (defence-in-depth) approach to information and cyber security controls to protect infrastructure and data.
- **Cyber security certification:** the maintenance of a suite of cyber security industry-recognised certifications and compliance memberships to implement best practice cyber security management processes and controls.

2.3 The University maintains information technology (IT) and cyber security standards to facilitate the effective implementation of cyber security controls and management across all IT infrastructure, systems and applications.

2.4 Standards are developed in consultation with key University stakeholders to support business requirements, provide adequate cyber security risk mitigation, and align with the cyber security framework.

Cyber Security Risk Management

2.5 The University identifies cyber security risk via a range of monitoring methods and addresses cyber security risks through a range of controls.

2.6 The Cyber Risk and Resilience team will maintain a register of key technology assets and cyber security risks, including with related controls.

2.6.1 These registers must be reviewed at a minimum annually, and also following any significant security incident, threat or change to business requirements.

2.7 The University must consider and assess the cyber security and privacy risks associated with all new activities that use the University's IT environment and when there is a change to existing activities. These risks must be assessed as part of the planning stages for these activities.

2.8 For IT environments that are not supported by the University (e.g. those hosted or managed by a vendor or third party), it is the responsibility of the University Contract Manager to ensure the system meets the University's information management framework and Cyber Security Standards and Baselines.

2.9 Staff must ensure that any contracts relating to the University's IT environment between the University and a vendor or third party are reviewed in accordance with the review processes of eSolutions and/or the Office of General Counsel.

2.9.1 Staff are only permitted to exercise a contract signing power as set out in the Authorised Financial Limits & Contract Signing Delegations Policy.

2.10 All contracts must clearly outline the vendor or third party's security responsibilities for storing or processing the University's information and the protection of the University's data. Contracts must include at a minimum:

- adequate consideration of cyber security based on risk;
- assurance to the University about the external systems cyber security risk management activities; and
- mandatory reporting to eSolutions of any actual or suspected breach(es) impacting or potentially impacting the information held in the University's IT environment, to be made as soon as practical after detection.

2.11 Third party users will be subject to confidentiality or nondisclosure agreements before being granted access to University IT systems and data.

2.12 System lifecycle management, such as commissioning and decommissioning of systems, software, and platforms is governed by eSolutions and must be undertaken in line with the appropriate security standards.

3. Information and Technology Management

3.1 The University's Information Management Framework facilitates identification, management and governance of information assets, and this underpins the cyber security framework.

3.2 The Information Management Framework mandates the security classification of information assets (both physical and virtual) and provides the basis for consistent, risk-based protection as set out in the Information Management Security and Classification Procedure.

3.3 The security classification of Information assets are managed according to the impact the University would incur in the event of an incident affecting any, or all, security attributes of the asset.

3.4 Users of University technology and systems must act in accordance with the Information Technology Acceptable Use Procedure. This includes:

3.4.1 engaging with IT resources responsibly and ethically while complying with University policies, procedures and schedules related to conduct, privacy, security, and data integrity; and

3.4.2 maintaining the security of their accounts and following security protocols and monitoring.

4. Security Awareness and Incident Management

4.1 The University promotes a positive security culture to improve its overall cyber security environment through education and staff training programs.

4.2 All staff must undertake mandatory cyber security awareness training, as set out in the Mandatory Compliance Training Procedure. Failure to complete mandatory cyber security awareness training may result in revocation of access to the University's IT environment.

4.3 A Monash authcate must be used when accessing University IT environments.

4.4 Staff and students should refer to the Cyber Safety Awareness website to facilitate the safe use of the University's IT environment.

4.5 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.

4.5.1 Online behavioural incidents, such as online bullying or threats, should be reported as per the Safety and Security Incident Reporting Procedure.

4.6 In the event of a cyber security incident, the University will follow the University Cyber Incident Response process to manage and comply with applicable legal requirements, minimise harm to impacted individuals, and minimise damage and risk to the University.

4.7 The University performs security testing against systems, processes and people to determine its vulnerability to cyber threats. The results of these tests will be used to measure and improve the management of the University's cyber risks and controls to prevent cyber threats.

5. Governance and Reporting

5.1 The Group Chief Information Security Officer (GCISO) is responsible for maintaining oversight of the University's cyber risk profile and ensuring active management of cyber risks.

5.1.1 Where a Monash University controlled or affiliated entity manages its own IT services and environments this responsibility lies with the Chief Executive Officer of that entity.

5.2 The Group Chief Information Security Officer (GCISO) is responsible for overseeing the implementation of cyber security controls, the management of cyber security incident response and development and maintenance of the University's cyber security strategy.

5.2.1 Where a Monash University controlled entity manages its own IT services and environments this responsibility lies with the Chief Executive Officer of that entity.

5.3 The University will make any report required by a government agency, and within the specified timeframe, including escalation of reports from parties received as per clause 2.10 in accordance with its legal obligations, on advice from the Office of General Counsel. This may include but is not limited to requirements that fall within:

- Australian Commonwealth reporting as per the Security of Critical Infrastructure Act 2018 and as per the Privacy Act 1988, and State reporting as per the Privacy and Data Protection Act 2014;
- European General Data Protection Regulation (GDPR);
- Indonesian Law No. 11 of 2008 regarding Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("Electronic Information Law"), Indonesian Government Regulation No. 71 of 2019 regarding provisions of electronic systems and transactions ("Reg. 71") and the Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System ("MOCI Reg 20/2016");
- Malaysia's Personal Data Protection Act 2010; and
- China's Cyber Security Law, Data Security Law and the Personal Information Protection Law.

5.4 The Cyber Risk and Resilience Team is accountable for the assessment of cyber security maturity, controls and control effectiveness as outlined on the University Cyber Security website.

5.5 Deans and Portfolio Heads are responsible for ensuring all staff they have oversight of comply with this policy and for facilitating the assessment of cyber security risks, and the implementation of cyber security controls in accordance with the University's Group Risk Management and Compliance Policy and the Mandatory Compliance Training Procedure.

5.6 University IT services and environments not managed by eSolutions, such as those managed by another Monash entity, vendor or third party, are required to complete an annual self-assessment of cyber security controls in addition to the report of any major cyber security incidents. These reports are to be made to and facilitated by the Cyber Risk and Resilience team.

5.7 Cyber security reports will be regularly provided to the Vice-Chancellor's Executive Committee (VCEC), Vice-Chancellor's Executive Implementation and Oversight (VCEIO) and the University's Audit and Risk Committee.

5.8 The University implements and maintains an ISO/IEC 27001 certified Information Security Management System (ISMS) for a specific scope of systems and their underlying infrastructure and operational processes, which are defined within the ISMS scope.

5.8.1 The ISMS will be supported by appropriate risk management practices and operational management resources, and will be utilised to ensure continuous improvement of the University's information security management controls.

6. Breach of Policy

6.1 The University treats any breach of policies, procedures or schedules seriously, it encourages reporting of concerns about noncompliance and manages compliance in accordance with the applicable Enterprise Agreement or relevant instrument of appointment or contract terms. A failure to comply with this policy 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.

6.2 Students found in breach of this policy may result in disciplinary action, in accordance with the Student Code of Conduct.

DEFINITIONS

Associate	For the purposes of this policy, 'associates' are defined as contractors, conjoint appointments, affiliates and adjunct appointees.
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
Cyber resilience	The ability for people, processes and technologies to quickly adapt to changing cyber threats.
Cyber risk	The potential of loss or harm related to technical infrastructure or the use of technology. Examples include but are not limited to:

	Phishing - scam emails: Phishing is a way that cybercriminals steal confidential information, such as online banking logins, credit card details, business login credentials or passwords/passphrases, by sending fraudulent messages (sometimes called 'lures'). **Malware** (short for 'malicious software') is software that cybercriminals use to harm your computer system or network. Cybercriminals can use malware to gain access to your computer without you knowing, in targeted or broad-based attacks. **Ransomware** is a type of malicious software (malware). When it gets into your device, it makes your computer or its files unusable. Cybercriminals use ransomware to deny you access to your files or devices. They then demand you pay them to get back your access. A **distributed denial of service (DDoS)** attack is an attempt to make an online service unavailable by overwhelming it with traffic. **Data spill:** Sometimes personal information is released to unauthorised people by accident or as the result of a security breach. For example, an email with personal information can be sent to the wrong person, or a computer system can be hacked and personal information stolen. These are known as data breaches or data spills.
Cyber Risk and Resilience	The capability within eSolutions that ensures effective management of cyber risk and resilience of technology across the global Monash University landscape.
Cyber security controls	Seek to reduce cyber security risk by either reducing the likelihood or impact of an incident, or both.
Cyber security incident	An event that results in a breach of explicit or implied digital security policy that requires corrective action as it threatens the confidentiality, availability and integrity of an information system or the information that the system processes, stores or transmits
Cyber security metrics	Metrics includes but is not limited to the current risk level, security control effectiveness and maturity of the University's approach to cyber security against best practice frameworks.
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 security attributes	The three principles of confidentiality, integrity and availability used within organisations to support the prevention of unauthorised access, use, disclosure, modification or destruction of information assets.
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.
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.
IT environments	For the purpose of this policy, 'IT environments' includes all IT infrastructure including electronic devices, hardware, software, networks, websites, systems and services owned or controlled by the University, or any University controlled or associated entity.
Monash authcate	An authcate (consisting of username and password) is the secured means for verified users to access Monash University information technology facilities and services enabled by single sign-on.
Risk assessment	The determination of quantitative or qualitative estimates of risk related to well-defined situations and a recognised threat.

GOVERNANCE

Supporting procedures	Domain Names Procedure Information Security and Classification Management Procedure Information Technology Acceptable Use Procedure
Supporting schedules	N/A
Associated policies	Group Risk Management and Compliance Policy

Related legislation	**Australia** Privacy and Data Protection Act 2014 (Vic) Health Records Act 2001 (Vic) Higher Education Support Act 2003 (Commonwealth) Higher Education Standards Framework (Threshold Standards) 2021 (Commonwealth) Epidemiological Studies (Confidentiality) Act 1981 (Commonwealth) - where relevant to a research project (needed) Public Records Act 1973 (Vic) Security of Critical Infrastructure Act 2018 (Commonwealth) Privacy Act 1988 (Commonwealth) **China** Cyber Security Law Data Security Law Personal Information Protection Law **Europe** General Data Protection Regulation (GDPR) **Indonesia** Law No. 11 of 2008 regarding Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("Electronic Information Law"). Government Regulation No. 71 of 2019 regarding the Implementation of Electronic Systems and Transactions ("GR 71") and Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data ("MOCI Reg. 20"). **Malaysia** The Computer Crimes Act 1997 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)	
Category	Governance	
Approval	Monash University Council 22 March 2023	
Endorsement	Audit & Risk Committee 15 March 2023	Vice-Chancellor's Executive Committee 28 February 2023
Policy owner	Group Chief Information Security Officer	
Date effective	1 April 2023	
Review date	1 April 2026	
Version	1.2 (*Administrative amendment effective 28 March 2025*)	
Content enquiries	cyberteam@monash.edu	