Cyber Security Policy and Procedure

1. Purpose

The purpose of this policy and procedure is to establish the Institute's cyber security risk management framework to prevent, reduce and manage compromised information security.

The Institute's approach to cyber security is informed by the Victorian Government *Protective Data Security Framework and Standards (VPDSF)* being the overall scheme for managing protective data security risks, and the Australian Government *Information Security Manual.*

2. Scope

This policy and procedure applies to all staff, students, third parties (partners, contractors, consultants, etc.) and visitors regardless of location or device ownership and includes any person or entity with authorized use of the Institute's IT systems, internet and/or email.

3. Definitions

Terms	Definition
control	Is a measure put in place to manage, minimize or eliminate risk.
Cyber security	the methods (policies, strategies, behaviours, and techniques) through which necessary and commensurate measures can be identified, implemented, and maintained to effect information security.
IT and Infrastructure	Is responsible for IT systems at the Institute. Noting that in addition to hosting IT systems at the Institute some facilities may be hosted externally.
IT systems	All services including data, voice, video, delivered through electronic means. Such technologies encompass systems, software, hardware, communications, and network facilities.

4. Policy

4.1 The Institute is committed to delivering information security by preventing unauthorised access to, and modification or impairment of, its digital IT systems and the information stored within them; through a combination of preventative measures, cyber security incident management, and the participation of all authorised users in ensuring that security measures are not undermined. *Cybercrime Act 2001 (Comm)*

The following Institute Cyber Security Strategy is adopted to proactively improve cyber resilience:

1. Application whitelisting - Whitelist approved and trusted programs to prevent the execution of unapproved or malicious programs from executing.
2. Patching applications - Perform regular patching/updating of applications in your network.
3. Office macros - Configure Microsoft Office products to block the execution of un-trusted macros.

4. Harden user applications - Tightly control applications that can perform unwanted or potentially vulnerable actions.
5. Restrict administrative privileges - Restrict administrative privilege for operating systems and applications based on user duties.
6. Patch operating systems – Routinely patch and upgrade your operating systems to the latest versions.
7. Use multi-factor authentication - Set up multi-factor authentication to provide higher authentication assurance for privileged, power, and remote user access.
8. Backup daily – Create regular backups of your most important data and configuration settings to help you recover quickly from a disruption. Keep backups on a device that is not connected to your network. *(VPDSF)*

4.2 Preventative measures are in place to provide control around the Institute's IT systems, including but not limited to:

- Firewall hardware and software to log and protect internet and network usage, including connectivity of all authorised users and IT systems, to prevent known threats and vulnerabilities from being exploited.
- Blocking of certain websites URLs, as their content is considered unsafe, unacceptable, or would put people, IT systems, or the Institute at risk. This includes, but is not limited to, malicious, gambling, pornographic, or terrorist content.
- Blocking of certain applications or limiting internet traffic to certain high bandwidth streaming applications to prevent an unnecessary drain on Institute IT systems.
- Using antivirus software to ensure the confidentiality, integrity, and availability of its IT systems and detect any malware or similar malicious code. Where possible, its source is traced.
- Automated Spam and Phishing detection to detect spam, phishing messages, and other malicious email entering and leaving Institute email servers, to protect against Spam, Phishing attempts, and viral outbreaks.
- Password strength requiring a certain level of complexity in all users' passwords.
- Identification and management of technical vulnerabilities
- Cryptography via digital certificates using a bona fide and valid Certificate Authority *(ISO 27002)*
- Awareness information and training.
- Monitoring of logs to detect signs of external interference.

4.3 Security controls at the Institute are based on a cloud security plan that:

- Ensure access to appropriately skilled resources to secure the service. This may involve training in-house staff or procuring specialist support.
- Incorporate appropriate Identity and Access Management based on roles, especially for administration duties.
- Ensure secure communications between users and the service.

- Establish a security control regime using third-party tools (Cloud Access Security Broker) to achieve better visibility, data security, threat protection and compliance, as well as to automate security configurations where possible.
- Take full accountability for application and data security in production, staging, development and test (non-production) environments and ensure roles and responsibilities are clear.
- Standardise all cloud deployments on 'hardened' images such as those available from Centre for Internet Security.
- Ensure that contracts support the ability to revert from the cloud. Clarify data sovereignty and the location of online and offline backups.
- Agencies should leverage existing security assessments where available for each contract.
- Ensure mechanisms are in place for the service provider to notify the Institute of cyber incidents and data breaches.
- Ensure regular independent security auditing of the service. This may be achieved under existing certification and accreditations such as ASD cloud or ISO27001 certification.

5. Procedure

5.1 The Institute's Cyber Security Strategy and preventative measures will mitigate risk and help protect critical information against cyber threats through compliance with this policy and procedure, and its local operating procedures, standards, guidelines, and systems. This includes technical cyber security controls and a cyber security awareness program to reduce vulnerability of staff and students to cyber security threats by fostering a culture that encourages cyber security.

5.2 Risk management will centre around cyber security controls that seek to reduce the likelihood or impact of an incident, or both. Cyber security risk management will be measured by:

- Maintaining a register of key information assets.
- Establishing a framework for performing cyber security risk assessments.
- Incorporating cyber security risk identification and assessment into processes impacting the use and processing of information.
- Maintaining a register of cyber security risks with related controls.
- Reviewing risks at regular intervals and due to significant security incidents, threats, or changes to business requirements.
- Implementing and strengthening controls to reduce risk.
- Evaluating the effectiveness of controls.

5.3 A cyber security incident is an event involving an actual or potential malicious actor that threatens the confidentiality, integrity, or availability of Institute information assets (electronic or paper) or otherwise contravenes this policy. The source of a cyber security incident may be accidental, malicious, or significant exposure to a known threat.

The Manager IT and Information will manage cyber security incidents by applying quick, effective, and orderly responses that aim to comply with applicable legal requirements (see

Notifiable Data Breaches Policy and Procedure), minimise harm to impacted individuals, and minimise damage and risk. Management of incidents includes communication and collection and analysis of evidence from the incident. All incidents must be reported to the Executive Management Committee and to the Audit and Risk Management Committee.

Controls and other preventative measures are put in place to avoid cyber security incidents, either because of experience from previous incidents or as a countermeasure or deterrent to likely incidents. These measures are documented and regularly reviewed to ensure their validity and reliability. (ISO 27002)

5.4 Cyber security vulnerability testing will be performed against systems, processes, and people to determine the Institute's vulnerability to cyber threats. The results will measure and improve service quality and protection against cyber threats.

6. Responsibilities

6.1 **Users**

Staff and students are responsible for reporting potential cyber security incidents to IT and Infrastructure support, including those of an accidental nature such as a lost laptop or device.

Staff and contractors are responsible for:

- Participating in cyber security training where relevant to their work role; and
- Acting consistently and responsibly to protect the Institute's information assets by –
- Complying with procedures in place to protect information assets;
- Incorporating safe cyber security practices into their work; and
- Reporting risks to IT and Infrastructure.

6.2 **IT and Infrastructure**

6.2.1 The Manager, IT and Infrastructure will assess the ongoing maturity of the Institute's cyber security practices and review this policy in response to significant cyber security incidents and changes in cyber security strategy and applicable legislation.

6.3.2 The Manager, IT and Infrastructure is accountable for the maintenance of cyber security metrics for reporting to the Audit and Risk Management Committee on a half-yearly basis. The metrics will cover the following cyber security management:

- current risk level;
- control effectiveness;
- the Institute record of cyber security against best practice.

6.3.3 The IT and Infrastructure Team will drive compliance with this policy and procedure through:

- ongoing cyber security awareness activities;
- checks in key IT processes to ensure cyber security risk management activities are performed;
- technical enforcement;

- regular reporting of self-assessments by Institute departments and Schools on required cyber security controls implemented to protect information assets; and
- audits to assess compliance and effectiveness of technical controls.

6.3.4 IT and Infrastructure Team manage relevant cyber security risks and are accountable for compliance with relevant cyber security standards and operating procedures including:

- Assisting to identify and develop suitable cyber security frameworks, standards and local operating procedures.
- Monitoring IT systems and services for potential cyber security risks and threats.
- Reviewing the effectiveness of cyber security controls.
- Reporting cyber security incidents to the Board of Directors through the Audit and Risk Management Committee (ARMC), together with an assessment of the operational effectiveness of cyber security controls at MIT. Such reports to be at least six-monthly, or immediately in the event of a serious cyber security breach.

6.4 Audit (internal and/or external) will provide independent oversight, review and assurance on the effectiveness of cyber security controls to manage risk and meet compliance requirements.

7. Implementation and Communication

The policy will be implemented and communicated throughout the Institute via:

- the Institute's webpage;
- Internal circulation to staff;
- Staff professional development.

Supporting Documents

Cybercrime Act 2001 (Comm)
Australian Government Information Security Manual
Victorian Government Protective Data Security Framework and Standards (VPDSF)
NSW Cyber Security Strategy
International Standard for Information Security, ISO 27002
MIT Notifiable Data Breaches Policy and Procedure
MIT Social Media Policy and Procedure