# Information Security Policy

## Audience and scope:

This policy is relevant to all staff, students and other users of computer systems owned or managed by Manukau Institute of Technology Limited (MIT).

### Document management and control

| | | | |
|---|---|---|---|
| **Policy Number** | ICT6 | **Consultation Scope** | Executive Leadership Team |
| **Category** | Management | **Approval Bodies** | Chief Executive |
| **Policy Owner** | DCE Operations | **Review Dates** | June 2024 |
| **Policy Contact Person** | Head of Technology Services | | |

### Amendment history

| Version | Effective Date | Created/Reviewed by | Reason for review/Comment |
|---|---|---|---|
| .001 | 19th March 2018 | Russell Smith | Created new policy. |
| .002 | 22nd March 2018 | Russell Smith | Review by Service Delivery and Legal |
| .003 | 26th April 2018 | Russell Smith | Review by Technology Services Management |
| .004 | 28th May 2018 | Jenna Woolley | Review by Executive Leadership Team |
| .005 | 6th May 2022 | Ricky Oliver | Review, update to reflect new Executive leadership structure |

# Table of Contents

# Information Security Policy

## Purpose

MIT has adopted the following Information Security Policy as a measure to protect the confidentiality, integrity and availability of Institutional information assets as well as any Information Systems that store, process or transmit these assets.

This policy will ensure that MIT's information assets are secured to the appropriate degree. These information assets are of significant value to the Institute. MIT is required under various legislation to retain accurate and complete records. If they are not available when needed or are improperly disclosed, MIT could incur serious loss of reputation and /or legal liability. Additionally, New Zealand legislation requires that the Institute protect student and staff privacy.

Sensitive information must also be safeguarded when in printed mode against unauthorised copying or disclosure by failing to store or destroy in the correct manner.

MIT has a zero tolerance to fraud. As well as seeking to reduce both the opportunity and scope for fraud, MIT is also committed to creating an environment where staff are able to freely report suspected cases of fraud and misconduct, and taking prompt action to fully investigate and address any suspected cases, whether carried out by staff, students, suppliers or other partners.

As such, MIT reserves the right to monitor, access, inspect or disclose information stored on or transmitted through MIT's information systems.

## Outcomes

This policy seeks to:

- Recognise the role of information security at MIT ensuring that users have access to the information they require to carry out their work.
- Avoid any reduction in the confidentiality, integrity or availability of information that could prevent MIT from functioning effectively and efficiently.
- Ensure there is no unauthorised disclosure of information that could potentially damage MIT's reputation and cause financial loss.
- Ensure users understand the importance of information security and, in particular exercise appropriate care when handling MIT's information, whether soft or hard copy format.
- Identify the process for recording and reporting any breaches of information security to the appropriate bodies both within MIT and externally.
- Ensure risk assessments on information security are performed on a regular basis identifying key information risks and determining the appropriate course of action to ensure risks are kept at an acceptable level.
- Apply industry best practice as the default position for all matters relating to information security. MIT base this default position on the Australian Signals Directorate (ASD) standard.

## Policy

### 1. Policy Content

This Policy applies to all Academic staff, Service staff and third-party agents of MIT as well as any other MIT affiliate who is authorised to access Institutional information assets. This policy is intended to ensure that the appropriate degree of access to and sharing of information assets will occur, and that academic freedom is protected.

1.1 All users are responsible for protecting MIT information from unauthorised access and use. This responsibility applies to both soft and hard copy format.

1.2 MIT confidential or commercially sensitive information must be protected, by the use of passwords and/or pin codes, from unauthorised access on any user's computer or portable device irrespective of whether the device is owned by MIT or the user. All users are responsible for protecting their MIT passwords and other access credentials from unauthorised use.

1.3 Applications and systems that contain MIT information must be properly disposed of so that the information cannot be retrieved or reassembled when no longer needed or required to be kept in accordance with the Archives New Zealand Standards and MIT's Records Management Policy.

1.4 MIT will conduct appropriate due diligence to ensure third parties who store or have access to MIT information are capable of properly protecting this information. Records of all such systems will be kept.

1.5 Any actual or suspected loss, theft, or improper use of, or access to, MIT's Information Systems must be reported to Technology Services, and MIT's privacy officer where relevant, as soon as practical.

1.6 All users must comply with MIT's Records Management Policy, in addition to the requirements outlined in this policy.

1.7 Misuse or disobedience of this policy may result in MIT taking disciplinary action in accordance with MIT's Disciplinary Policy HR7.

### 2. Responsibilities

2.1 Shared responsibility for Information Security rests with **all** staff, students, visitors and contractors to MIT.

2.2 Management of MIT are responsible for;

- Ensuring best practice information security is followed.
- Ensuring all staff, students, visitors and contractors are informed of and adhere to the Information Security Policy.
- Promoting clear desk practices, ensuring printed information is stored in a secure manner.
- Ensuring staff, who disclose information about fraudulent activity, are protected and can do so without fear of reprisal.
- The classification of data to ensure sensitive information (both hard and soft copy format) is disposed of in a secure manner.

2.3 Technology Services are responsible for;

- Establishing, directing and co-ordinating MIT Information Systems programme.
- Reviewing and reporting departmental compliance with this policy.
- Providing a single point of contact for oversight of serious information security incidents.
- Establishing information security metrics, tracking the progress of the Information Security Policy (against the ASD standards) and providing an Institute-wide IT risk profile.
- Ensure new Information Systems conform to information security standards before being installed into any production environment.
- Ensuring Information Security standards and requirements shall be included in product specifications during the procurement process.
- Ensuring that all infrastructure technology managed by Technology Services is protected against improper access.
- Ensuring systems and applications are kept up to date on all devices that process or store MIT information.
- When changes are made to systems that may affect the security of information assets, assessing risks, and ensuring that the system subsequently conforms to information security standards.
- Ensuring availability of appropriate information, education and training.

2.4 Users of MIT systems and confidential information have responsibility for;

- Keeping their MIT user credentials secure, this includes and keeping passwords private and not sharing passwords with others (no passwords should be written down).
- Ensuring all MIT information is stored on secure systems, sensitive information is stored with restricted access or password protection.
- Reporting any potential and suspected breaches of Information Security to Technology Services.
- At the end of employment (or contracted term, if applicable) with MIT, the return of all supplied equipment and property that contains or allows access to MIT information. Users shall not retain, give away, or remove from MIT premises any protected information.
- Ensuring work areas are, as far as conveniently possible, to be kept clear of papers in order to reduce the possibility of unauthorised access and loss of information during and outside normal working hours.
- Ensuring sensitive information in hard copy is stored in a locked drawer or cabinet when work areas are unattended.
- Destruction of sensitive information. Both hard and soft copy information must be disposed of in a secure manner.
- Ensuring no sensitive information is left unattended in a print area.

Ensuring suspicions of fraud, corruption or related misconduct are reported to through the appropriate channel.

## 3. eSignatures

3.1 All Users that apply eSignatures must do so in accordance with Clause 4 of MIT's Acceptable Use Policy (ICT1).

3.2 In all cases, the use of eSignatures by any user other than the Owner of the eSignature ("the Owner") should be kept to the minimum number of users necessary. Access to eSignatures should be treated as privileged access.

3.3 Users that have access to others' eSignatures must only access these for the purposes of carrying out their role and in accordance with MIT's delegated authorities, e.g. where appropriately authorised, to apply to documentation or for the printing of Academic Awards. This includes the following provisions:

a. With regard to documentation, where the user is not the Owner, users must:
   - Ensure the Owner has the appropriate Delegated Authority to sign the document.
   - Ensure they obtain written permission from the Owner to apply the signature in each separate instance and keep a secure record of that permission.
   - Provide evidence of written approval should it be required.

b. With regard to the Award of Qualifications, where the user is not the Owner, users must:
   - Obtain permission from the Owner by virtue of the confirmation of Awards through MIT Board proceedings.

Ensure the eSignature is applied in accordance with all Academic Registry procedures

## Procedures

## Evaluation/Outcomes

**Audit:** The Risk and Assurance Manager may audit compliance with this policy as part of internal audit work programmes.

**Compliance:** The policy owner will monitor compliance.

## Additional Information

### Glossary

| Term | Definition |
|---|---|
| Australian Signals Directorate (ASD) standards | The Australian Signals Directorate (ASD) provides information and IT security advice and assistance and is broadly applicable to businesses and other organisations. It is regarded as the Commonwealth authority on the security of information. |
| Availability | The state of an information asset being accessible to those individuals or systems authorised to access it when needed. |
| Clear desk policy | A directive that encourages employees to clear their desks of sensitive and confidential documents, when they leave the office at the end of the day. This also includes keeping sensitive and confidential material out of public sight, while at work. |
| Confidentiality | The protection of sensitive or private information assets from unauthorised disclosure. |
| Information Asset | Information assets are data, information, knowledge or expertise in any form stored or available on Information Systems. They may include financial, operational, or scientific information; student, staff or stakeholder related information; or strategies, processes, or research and development. |
| Information Security | Assurance that the confidentiality, integrity and availability of information assets and information systems are maintained to the appropriate degree. |
| Information System | Any electronic system that stores, processes or transmits information. |
| Integrity | The accuracy, completeness and validity of information. Integrity also means that an information asset has not been modified without authorisation. |
| Management | For the purposes of this policy, the term “Management” is used to refer to all persons in Line Management roles as well as those who are direct reports to the ELT and Directors of School and Performance. |
| Risk | The potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset |
| Risk Assessment | A systematic process for identifying the degree of risk to an asset. Assets are identified and their value assessed, threats are qualified, vulnerabilities are documented, potential consequences of a loss are described, and a determination of resulting risk and commensurate controls is produced. |
| Threat | Anything that could adversely affect an information asset. |
| User | Anyone using MIT’s information system. |

### Exemptions and dispensations

Any dispensations from the requirements of this policy, including one-off circumstances, must be approved in writing by the Chief Executive and forwarded to the DCE Operations

## Delegations

Board Delegation to the Chief Executive to determine management policies of the Institute in relation to the implementation of its approved Investment Plan and Strategic Plan and the management of its affairs (Board Register of Permanent Delegations CE/OP6).

## Relevant Legislation

- Copyright Act 1994.
- Privacy Act 2020.
- Education and Training Act 2020.
- Official Information Act 1982.
- Public Records Act 2005.
- Films, Videos and Publications Classification Act 1993.
- Protected Disclosures (Protection of Whistleblowers) Act 2022

## Legal Compliance

This policy complies with MIT's statutes, regulations and relevant legislation.

## Associated documents

The following documents are associated with this policy:

- Student Misconduct Policy (AM6).
- Intellectual Property Policy (AM10).
- Disciplinary Policy (HR7).
- Fraud Prevention and Response Policy (LC2).
- Protected Disclosures (Whistleblower) Policy (LC3).
- Protected Disclosure Process Guidelines.
- MIT Fraud and Corruption Procedure.
- Records Management Policy (LC4).
- Information Act Requests Policy (LC5).
- Privacy Policy (LC6).
- Acceptable Use Policy (ICT1).
- Australian Signals Directorate (ASD) standards.
- Archives New Zealand standards.
- Protected Disclosure Process Guidelines.
- MIT Fraud and Corruption Procedure.