MELBOURNE INSTITUTE OF TECHNOLOGY

User Account, Email, Internet Security and Management Guidelines

Table of Contents

1. Purpose

In accordance with the MIT Quality Assurance Framework, this Guideline serves to meet government legislation and statutory regulation requirements such as Education Services for Overseas Students Act 2000 (ESOS), National Code of Practice for Providers of Education and Training to Overseas Students 2018 (NCP), Higher Education Standards Framework (HESF); the MIT Framework for Secure and Confidential Information; and, MIT Strategic Risks relating to ICT infrastructure and systems.

2. Scope

The Guidelines are applicable to all staff and students.

The Guidelines is designed to serve as the induction/ orientation point for new staff and students, for over the counter enquiries and systems helpdesk matters. The IT&ID (Information Technology & Infrastructure Division) handles a broad range of student and staff technology. An overview of services provided by IT&ID is available via MIT website at:
http://www.mit.edu.au/students/Information-Technology-Resources
The IT&ID ensures that secure access to electronic information and adequate electronic communication services is available continuously (allowing for reasonable outages for maintenance) to students, staff and other relevant stakeholders during periods of authorised access, except for locations and circumstances that are not under the direct control of MIT.

3. Organisation Overview

The Melbourne Institute of Technology (MIT) was founded in the 1990s and has taken a measured approach to increasing its student profile over this period. The Melbourne Institute of Technology is an affiliated institute of Federation University Australia and also delivers a range of their undergraduate and postgraduate programs at its Melbourne and Sydney campuses. MIT has been offering higher education options for over two decades and in recent times has focused on increasing its own cohort of students and developed internal capacity to support them. With this, MIT has also been focused on building a team to support this growth.

> The principles underpinning MIT's approach to workforce planning are informed by the Institute's values and recognition that people are the most important resource in the education sector.

This is exemplified in MIT's value statement which commits to:

A. Excellence.
   - **Excellence in learning** - engaging our students through small class sizes, face-to-face student, and staff consultation, and making our students' aspirations, experience, needs

and feedback fundamental to evaluating our performance and driving continuous improvement.

- **Excellence in teaching** – through outstanding learning environments, offering industry relevant curricula, combined with academic rigor including recruiting and retaining highly qualified staff.

B. **Integrity.** Conducting ourselves with honesty, transparency and the highest ethical standards in all aspects of our activities and holding to these standards for our staff and students alike.

C. **Accountability**. Being accountable to our students, staff, each other, and to relevant industry bodies by adopting best practice in academic and corporate governance.

D. **Transformational Change**. Providing effective and innovative teaching methods and a diverse range of student support services to enhance our students' learning experience and opportunity for success.

Goals and Priorities:

- Develop and deliver innovative programs that meet industry and market needs;
- Provide an inclusive, service-oriented culture focused on student outcomes;
- Raise our profile and the impact of our teaching and learning and student engagement with our stakeholders;
- Provide inclusive, innovative and responsible education

Enabling Elements:

- Our people
- Technology

4. Information security

A. Information is an asset and like any other business assets it has value and must be protected.

B. The systems that enable us to store, process and communicate this information must also be protected.

C. An information system is the collective term for our information and the systems we use to store, process and communicate it.

D. The practice of protecting our information systems is known as information security.

E. Information security is managed by the IT Lead Systems Engineer/Systems Administrator and his team and approved by MIT Management.

F. All users of MIT systems are obligated to act in accordance with these guidelines except where specifically mentioned within these guidelines.

4.1. The Right to Monitor

MIT has the right to monitor the use of its IT services to maintain technical security and operational efficiency.

1. Suspected breach of policy will in all cases be brought to the attention of the Group General Manager and may be monitored.
2. Inspection of personal information will be undertaken in accordance of the Privacy legislation and only after approval by the Group General Manager.
3. Electronic data, information and material created by authorised users will be treated as confidential during monitoring.
4. Access to such information will be strictly on a need-to-know basis for technical or administrative purposes.
5. Incidental awareness of personal may occur through normal support operations. In such cases all information will be treated as confidential, except where such raises suspicion of breach of policy, in which case the matter will be brought to the attention of the Group General Manager per point 4.1.1.

5. Enforcement

1. MIT will not act as censor of information on MIT's network, but will investigate properly identified allegations arising from the member/users to ensure compliance with applicable laws and with MIT's policies and procedures.
2. Misuse of MIT's computing and network resources may result in disciplinary action by MIT. Illegal or harmful activities will result in immediate loss of privileges and may be reported to the appropriate MIT staff and law enforcement authorities.
3. Staff violations will be handled in accordance with the MIT's approved Employee Manual - Disciplinary Procedures. In most instances of unacceptable behaviour or misconduct, disciplinary action will progress in steps from reprimand to discharge, consistent with the employee's prior disciplinary record and the seriousness of the offence.
4. Student violation will be handled in accordance with MIT's approved Student General Misconduct Policy and Procedure.
5. In either case, access privileges may be revoked immediately and long-term outcomes may include temporary or permanent loss of privileges, depending on the nature of the activity.

6. User name and Password

6.1. Things you should know

1. Your username and password are essential to access MIT resources.
2. Your password will expire and need to be changed every 180 days.
3. If for any reason you fail to change your password within 180 days as prompted, you will not be able to log on to MIT's System.
4. Username and password used in Full time staff computer network (MIT Domain) and academic network (MITACADEMIC Domain) are separate entities.
    a. Changing a password on one does not change the password on the other.
    b. You need to change passwords in both networks.
5. Students and sessional staff should set up their password before the first time they are accessing the MIT systems or online portals by resetting it at MIT Self Service Password (https://passwordreset.mit.edu.a).

6. If you are having difficulty authenticating, please contact the IT Service Desk for help.

6.2. Things you should do

All users must ensure their password conforms to the following rules:

1. Does not contain your username or parts of your full name that exceed two consecutive characters

2. Contain characters from three of the following four categories:
   - ✓ English uppercase characters (A through Z)
   - ✓ English lowercase characters (a through z)
   - ✓ Base 10 digits (0 through 9)
   - ✓ Non-alphabetic characters (for example: !, $, #, %)

Please also note that:

- Complexity requirements are enforced when passwords are changed or created.
- A minimum password length of ten (10) characters is also enforced in the staff domain.
- A minimum password length of eight (8) characters is also enforced in the academic domain.
- Users cannot use previous 5 passwords.

6.3. Things you should not do

1. Do not share your password with others.
2. Do not write down your password in a place where other people can easily find.

7. Email usage

7.1. Things you should know

1. E-mail services are provided to the individual staff or student member only, and are not to be shared.
2. Email services are provided for use within the scope of the individual's role, and is not for personal use.
3. Full time staff (@mit.edu.au) incoming and outgoing emails are saved on the server, as well as backed up in various locations, and are accessible by MIT at any time.
4. Emails to and from subdomains (@stud.mit.edu.au & @academic.mit.edu.au) are stored only on the respective email server.
5. MIT emails remain the property of MIT at all times.
6. SPAM is any unsolicited or fraudulent emails. If you are not sure about the sender of the message or attachment, please do not open it, as it can potentially compromise our files, computers and network.
7. Disciplinary action will be taken if you fail to obey email usage rules.

7.2. Things you should do

1. While communicating with external clients (via email) you have to be 100% sure that the information is correct. Remember the information you are giving is on behalf of MIT. The company is liable for all information that is disseminated externally and internally. There are legal implications if the information is not correct.
2. Depending on the degree of importance, you must CC your IMMEDIATE SUPERVISOR or consult with him or her before e-mailing.
3. Ensure that you use web-based email facility for your personal email correspondence e.g. yahoo, Hotmail, Gmail and access these services outside working hours and not at MIT.

7.3. Things you should not do

1. Do not send any spam messages through MIT's Network
2. Do not attempt to circumvent mailbox security for malicious intent or any reason.
3. Do not attempt to access mailboxes which you are not authorised to access.
4. Do not send/copy MIT emails to unauthorised email addresses including employee private email addresses.
5. Do not forward emails which you believe contain virus or malware.
6. Do not open email attachments from unknown or suspicious sources.
7. Ensure that email must not be used to humiliate, intimidate or offend another person or persons on the basis of their race, gender, sexual preference, disability or any other attributes prescribed under anti-discrimination legislation.
8. Staff are not to delete MIT business email per the Records Management Policy and Procedure.
9. Staff will ensure that they have Signature attached when sending email. Please call IT helpdesk if you do not have this.
    a. ***For example***;

    Full Name | Position
    The Argus, Level M, 284-294 La Trobe Street, Melbourne Victoria 3000 Australia
    t: reception +61 3 8600 6700 | f: +61 3 86006799|t: direct +613 8600 6715 |
    email: email@mit.edu.au
    w: www.mit.edu.au | tw: twitter.com/mitaustralia | fb:
    facebook.com/mitaustralia | Skype: melbinsttech

8. Internet Access

8.1. Things you should know

1. Internet usage is logged and reviewed periodically.
2. Certain sites are blocked and can only be opened in the event where such access is required for work purposes.
3. Internet is shared usage and bandwidth limits are in place to allow fair use.

8.2. Things you should do

1. Take extra care while accessing sites or online services.
2. When prompted as in the case of various websites to download materials always select "NO", unless such websites or sources are trusted sources.

8.3. Things you should not do

1. Do not use this facility for your personal benefit.
2. Never use this facility to harm other people or systems in any way.
3. Never try or access sites or participate in illegal downloading or distribution of copyrighted materials.
4. Do not attempt to bypass firewall content filtering by using proxies, VPN or similar technologies.

9. Personal and Shared Drives (H: and J:)

9.1. J Drive (Full Time Staff Only)

Full time staff members are provided access to a share drive (J:) where they can share work with other staff members. Staff require authorisation to access folders stored in the share drive from their immediate supervisor.
Staff members require re-authorisation by the immediate supervisor if the user was removed for any reason. Authorising staff members are required to request in writing, the removal of any staff members access from the share drive or folder.

9.2. H Drive

- All users are provided with a Network Drive (H:) for data to be stored
- H drive is backed up on a daily basis
- Any other drives such as C are not backed up and any data stored on a computer which has malfunctioned may be lost.

10. Securing Personal Information of students

In accordance with Australian law, MIT is responsible for securing the personal information that we store about our students. This includes the information stored in MIT systems (Bigfoot and others) and also physical documents. Several security strategies are in place to secure this information including but not limited to:

- Staff are unable to print or copy without using their ID card or PIN.
- Secure passwords are needed for accessing IT systems.
- Audit logs of who accessed what systems and information are kept.
- IT accounts of users who are no longer associated with MIT are disabled and/or removed.
- Secure login for services such as Moodle via SSL certificates is required.
- Secure VPN connection for staff working remotely is logged
- Antivirus and Malware protection software and hardware is installed to protect systems.
- Enterprise grade firewall with advanced security features are utilised.
- Proper access controls mechanisms and management across all MIT systems.

11. Storage of MIT business files (Staff only)

All files & data created while working at MIT remain the property of MIT. As such, staff are held responsible for ensuring that proper data storage practices are maintained.

11.1. Things you should do

- Staff must ensure to use the supplied network drives (J: & H:) for the storage of all MIT business documents.
- Staff should organise their files such that unnecessary duplicates of files and folders are created, and that they may be easily traversed.
- Staff must take every step to ensure no unauthorised access to MIT business files occurs.
- Staff may use other storage mediums, provided that the above 3 points are met.

12. Software and its usage

12.1. Things you should know

- MIT does not provide software for personal use unless specifically granted by the software vendor to do so. Most exceptions are by way of vendors sites where applicable.
- MIT provided software is licensed to be installed and used in MIT's computers only.
- At no stage will local administrative privileges be granted to an MIT user, unless with express approval of the Group General Manager.
- The IT&ID will keep track of all the software installed on all workstations/portable computers for compliance reasons.
- MIT will not take responsibility for any software that is not installed by IT&ID or approved by IT&ID, i.e. you will be personally liable for any damages that such installation may cause.
- If you require software that is not part of the standard software issue/installation, you will be required to:
  - Contact IT&ID with the reason of why you require that particular software.
  - If MIT already has the software that you request, the IT&ID will install it for you.
  - If MIT does not have the software requested, you can make a request via your line manager for the software.
- If management approves the Software purchase, the IT&ID will install the software for you.
- Do not change any registry settings for the computer without authorisation.
- Do not delete any software folders from your computer.

12.2. Academic Management System (AMS)

The IT&ID provide first level support for the AMS. Academic Management System – AMS is a portal that provides staff and students with access to resources and tools for the collection, collation and dissemination of information regarding enrolments, timetables, assessments and timesheets.

12.3. Bigfoot (Staff Only)

The IT&ID provide first level support for Bigfoot. Bigfoot is a database that stores and manages student records. IT&ID will escalate Bigfoot problems to the Bigfoot administrator when necessary.

12.4. Moodle

The IT&ID provide first level support for Moodle. Moodle is the MIT learning management system. IT&ID will escalate Moodle problems to the Moodle administrator when necessary.

12.5. ELO (Staff Only)

The IT&ID provide first level support for ELO. ELO is a database that stores and manages student files in electronic format. IT&ID will escalate ELO problems to the vendor administrator when necessary.

12.6. Greentree (Staff Only)

Greentree is the staff leave management portal, which is managed solely by the finance department. The IT&ID does not provide support for Greentree.

12.1. Turnitin

MIT uses Turnitin to promote academic integrity and deter plagiarism. The IT&ID provide first level support for Turnitin such as creating accounts.

12.2. Web SMS (Staff Only)

Online SMS services are available to authorised staff members.
While using this service all staff members are required to at all times:

- Have authorisation in writing from the Group General Manager to use this service.
- Not send SPAM. This behaviour will result in disciplinary action being taken.
- Not harass, intimidate or threaten another person or persons.
- Not send sexually explicit material, even if it is believed that the receiver will not object.

12.3. Zoom

Zoom is a high-quality video and audio online conferencing tool for desktops, tablets and smartphones. Zoom Meetings are ideal for online classes, meetings, special events, webinars, distance learning, group work, breakout rooms, collaboration, research supervision and collaboration, mentoring and even job interviews. IT&ID will escalate Zoom problems to the Zoom administrator when necessary.

13. Borrowing IT equipment

IT equipment refers to, but is not limited to items such as laptops, mobile phones, audio-visual (projectors), computers, printers, routers, switches and cables. This includes allocated devices such as laptops and tablets. In all cases, such will remain the property of MIT and will remain under the jurisdiction of IT&ID.

Where not specifically allocated, Staff members requesting to borrow MIT IT equipment for private or work-related purposes are required to follow the procedures:

- Authorisation in writing from management 48 hours prior to use.

- All equipment must be signed out by the borrowing staff member.
- All equipment is to be returned in its original state.

By signing out the equipment, the staff member accepts all of the following:

- The IT&ID is not liable for any damage caused in the process of such use.
- The staff member will be held liable for any damages, loss or theft during such use.
- That borrowing of IT equipment is a privilege and requests may be refused.

14. Installation / Set up of IT equipment

Staff members requesting set up or installation of IT equipment must at all times follow the procedures as follows:

- Where a setup is normally scheduled as a part of operations, i.e. o-week, graduation, IT&ID will confirm the planned deployment and any changes necessary at least two weeks prior to the setup with the authorised/delegated event leader.
- Where the setup is not normally scheduled, authorisation in writing from management is required at a minimum of 2 weeks prior for items that will be used for events such as meetings etc.
- Any request outside these times will be met with best effort, however there is no guarantee that a setup will be able to cover all needs. As such, please give IT&ID as much notice of requirements as possible.
- In all cases, the requesting staff member is responsible for arranging rooms, tables and any other non-IT equipment required prior to set up / installation.
- The requesting staff member is responsible for the safe-keeping of any IT equipment.

15. MIT Telephone Facility (Staff Only)

- All phone calls from the telephone stations and computer applications (such as MS-Teams) are restricted according to the users work requirements.
- Authorisation is required for accessing restricted services such as international calling.
- Do not use this service for your personal benefit.

16. Printing/Photocopying/Fax Services

- Printing, photocopying and fax services facilities are shared.
- Colour printing and photocopying is available to staff upon approval from management.
- Individual staff printers are issued to users who use printers extensively, on the approval of the Group General Manager.
- Staff are not to use MIT's printing, photocopy and faxing services for personal use.
- The IT staff provide first level support for all of the printers
- Students are responsible for their own printing. Student print credit is pre-payable, and wholly the responsibility of the student. Students are not limited in their printing in any way outside of it being charged.

17. Storage and Data Recovery

- Data stored on MIT's network and used by server applications are backed multiple times over the course of the day, and are retained indefinitely. However, this does not mitigate the end user's responsibility in maintaining all email and proper records management practices.
- If a user inadvertently deletes a file from a network drive staff requesting the return of a deleted document or email will be pointed towards the Records Management Policy and Procedure. Staff are reminded to be aware of their obligation in meeting this policy.
- The IT&ID have a data recovery plan in case of disaster.

18. Support requests

All IT support requests are recorded and managed via our KACE online IT ServiceDesk. Users may raise any issue by:

1. Emailing servicedesk@mit.edu.au directly
2. In-person at the IT support helpdesk of each campus

Associated Documents

MIT Associated Documents

MIT Quality Assurance Framework,
http://www.mit.edu.au/about-us/governance/institute-rules-policies-frameworks-and-plans/Frameworks/QualityAssurance

MIT Employee Manual,
https://online.mit.edu.au/ams/UserFiles/file/MIT_Employee_Manual_2018.pdf

Academic Staff Supplement to Employee Manual,
https://online.mit.edu.au/ams/PublicDocs/Academic-Staff-Supplement-to-Employee-Manual-2019T2-v3.pdf

Critical Incident Policy and Procedure,
http://www.mit.edu.au/about-us/governance/institute-rules-policies-and-plans/policies-procedures-and-guidelines/MIT_Critical_Incident_Policy_And_Procedure

Privacy Policy,
http://www.mit.edu.au/privacy

MIT Records Management Policy and Procedure,
http://www.mit.edu.au/about-us/governance/institute-rules-policies-and-plans/policies-procedures-and-guidelines/MITRecordsManagementPolicyAndProcedure

Student General Misconduct Policy and Procedure,
http://www.mit.edu.au/about-mit/institute-publications/policies-procedures-and-guidelines/MIT-Student-General-Misconduct-Policy-Procedure
MIT website,
http://www.mit.edu.au/students/Information-Technology-Resources

Legislation Context

TEQSA (Tertiary Education Quality Standards Agency)

TEQSA Guidance Note: Staffing, Learning Resources and Education support

Higher Education Standards Framework 2015 (HESF)

HESF Domain 2: Learning Environment

ESOS (Education Services for Overseas Student Act 2000)

NCP 2018 (National Code of Practice for Providers of Education and Training to Overseas Students)

Document information

Document Title	User Account, Email and Internet Security and Management Guidelines
Version	1.6
Approved Date	10/09/2021
First Issued	6 March 2013
Review Date	10/09/2023
Maintained by	MIT IT Infrastructure and Services

Revision History

Version	Date
1.4	05/03/2018
1.5	02/01/2020
1.6	09/09/2021