Records, Data and Information Management and Security Policy

Supporting plans, policies and procedures	• ICT/Infrastructure Plan • Privacy Policy • Critical Incidents and Business Continuity Plan • Equity, Diversity and Aboriginal and Torres Strait Islander Peoples Framework and Policy • Conferral of Awards and Graduation and Academic Documentation Policy • Academic Progress and Student At-Risk Policy and Procedure • Academic Assessment and Moderation Policy and Procedure • Code of Conduct • Freedom of Intellectual Enquiry Policy • Marketing and Student Recruitment Policy • Risk Management Policy • Critical Incidents and Business Continuity Policy and Procedure • Facilities, ICT Infrastructure and Resources Policy
Related legislation and references	• Higher Education Standards Framework (Threshold Standards) 2021 • Tertiary Education Quality and Standards Agency (TEQSA) Act 2011 • Australian Privacy Principles
Version	3.0
Approved by	Board of Directors and Academic Board
Date approved	23 July 2021
Document Review	This document is to be reviewed every two-years at a minimum from the date of final approval

Version	Review Date and Person/Body	Notes
0.1	Draft prepared by CEO and approved at 7 January 2020 Board of Directors meeting	
1.0	Reviewed by Learning and Teaching Committee (LTC) on 4 February 2020	
1.1	Presented to Academic Board on 18 February 2020 for review and approval	The Academic Board requested reference to the Privacy Principles and definitions of who's accountable for different data be added
1.2	Presented to Academic Board on 21 April 2020 for review and approval	Included items requested by the Academic Board on 18 February 2020
2.0	Approved by the Academic Board on 21 April 2020	Included items requested by the Academic Board on 21 April 2020
2.1	Reviewed and approved at 20 October 2020 Academic Board meeting	Minor amendments following comments from external reviewers
	Reviewed and approved at 28 October 2020 Board of Directors meeting	
3.0	Reviewed and approved by the Board of Directors and Academic Board via email circulation on 23 July 2021	Updates made following the response to the TEQSA Request for Information 23 July 2021

Background and Scope

This policy defines how MIHE manages data collection, retention, security and destruction of records. This policy applies to all directors, committee members, staff, students and contractors. This policy applies to all records, data and information created or received in any format to support MIHE operations. Also, refer to the *Privacy Policy* which was developed in alignment with the Australian Privacy Principles (APP) guidelines provided by the provided by the Office of the Australian Information Commissioner. (https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/)

Definitions

Data	Data means information, resources, and other records that fit into one of the following categories: • Public Access - data that is publicly available and is unlimited in access to all students, staff, and the general public such as the MIHE's public website • Internal Data - data used and accessed only MIHE staff and not to be used by external sources without prior approval • Internal Protected Data - data that is only accessible by the staff members that are required to use it to complete their assigned duties at MIHE • Internal Restricted Data - secure data that is to be kept confidential with specialised authorisation that must be given to anyone wishing to access this type of data

Also refer to Glossary of Terms.

Policy

MIHE is committed to meet its legal obligations by administering its data, information and records in a lawful, ethical and cost-effective manner. This policy sets out the guidelines for all MIHE staff to abide by at all times to ensure the safety and security of all records and data collected by MIHE. MIHE is the sole owner of all data and no one individual will ever be in complete control of any type of data associated with MIHE. All MIHE staff will perform the essential role of record keeping.

A Data Leader at MIHE will be in charge of ensuring that there is appropriate data quality and security and that this policy is appropriately being adhered to. The Data Leader in charge of any piece of data is responsible for allowing the access and distribution of that specific set of data in accordance with MIHE's policies and procedures.

The Data Leader also has the following responsibilities:

- Determining whether or not any individual should be granted access to a piece of data that is otherwise considered to be protected or restricted. When the Data Leader does not have the

ability to grant access alone, they must work together with their supervisor or the appropriate staff before permission can be given to access the data.

- Consider and assess the reason for the data access request along with what the data will be used for after access has been granted (see Data access and disposal section of this policy) for details.
- Ensure all appropriate steps below are completed to ensure that records are as accurate and complete as possible:
  - Plan, design, capture and develop data/records collection
  - Organise, store and protect data/records
  - Apply, monitor, review, improve and/or dispose of data/records.

In addition to the Data Leaders, all data users are responsible for making sure that the appropriate steps and guidelines are followed when accessing data to ensure the value and reliability of the data/records remain intact and useful to future data users. Data Leaders and all data users must also adhere to all of MIHE's policies and procedures, including the *Privacy Policy*.

All data records must be kept current. This is to include updates done at every step, in both audible and visible formats.

To ensure that the security and safety of data are never at risk either intentionally or unintentionally, the use of any data for personal use is always prohibited. Also, before any data other than public data is used, collected, or shared there must be prior approval given by the Data Leader or MIHE's Chief Executive Officer. Where the data is to be collected used or shared for academic purposes, approval may be given by the Data Leader or suitable academic staff member.

Electronic safeguards must be in place for all data stored on electronic sources. Hardcopies must also be stored in a locked drawer or any other manner that ensures that each is protected from access by unauthorised individuals. Hardcopies must not be altered, and all care must be taken to prevent from damage. *Critical Incidents and Business Continuity Policy and Procedure* outlines process for managing potential loss of records.

All data should be disposed of properly and as required securely. Hard copies and electronic sources (such as hard drives and flash drives) will be disposed of in secure destruction bins. All hardcopy data and records may be retained or archived for up to seven years. All electronic Student Data is to be retained permanently (as shown in the tables below).

Data Access and Disposal

Staff may have access to those records necessary to fulfil their duties at MIHE. However, access to certain confidential record may be restricted. All organisational data will be kept on site unless there are compelling circumstances (such as a legal requirement) which require their release or transfer,

or are required for data backup and other needs as part of the *Critical Incidents and Business Continuity Plan*. External parties will not have access to records unless authorised by the Data Leader or required by the law. Any staff member who receives a request from an external party for access to any record should seek for approval from the Data Leader before sharing any information.

The following tables outline the key data, including registers, that MIHE manages, including data source, data type, data form/system, data leader and data disposal requirements.

Data in the following table have the following data disposal requirements:

- Hard copies securely destroyed within seven years when electronic copies exist. Paper records should be disposed of using the secure shredding bins provided.
- Electronic copies and data retained permanently (especially for all student data)

Data Source	Data Type	Systems	Data Leader
Student enrolment, progression, completion, qualification and award data	Internal Restricted	Student management system	Dean, Administration Manager
Student feedback and survey information			
Course delivery material: outlines, study guides, reading guides Course guides – course descriptions, requirements, content, outcomes Assessments, examination questions		Hardcopies, Electronic copies stored on secure network server, Moodle	Dean, Course Director
Corporate Documents (policies, plans, insurance policies, etc.)	Public Access, Internal, Internal Protected, Internal Restricted	Hardcopies, Electronic copies stored on secure network server	CEO, Dean, Administration Manager

Data that does not fall into any of the categories in the table above will have the accountable Data Leader as per the following definitions:

- The Dean is the accountable Data Leader for all student and academic data.
- The CEO is the accountable Data Leader for all MIHE data except student and academic data (which is the accountability of the Dean).

The data in the following table have the following data disposal requirements:

Electronic copies and data retained permanently (especially for all student data).

Registers	Data Type	Systems	Data Leader
Complaints Register	Internal Restricted	Electronic copies stored on secure	CEO, Dean, Administration Manager
Academic Misconduct Register			
Non-Academic Misconduct Register			

Critical Incident Register		network server	
Conflict of Interest Register			
BoD and AB Resolutions Register			
Policies and Procedures	Public Access, Internal, Internal Protected, Internal Restricted		

Auditing

Records, data and information management activities and practices will be audited regularly, under the oversight of the Audit and Risk Committee (ARC), to ensure security and compliance. Auditing will ensure accuracy and fairness of MIHE's records, data and information management systems.

Penalties

Breach or failure to comply with this policy may result in disciplinary action in accordance with the *Code of Conduct*.