Policy Title:	MIE IT Information Security Policy
Description:	This Policy outlines the operation of Security Standards on the MIE Network
Author (Position):	Director of IT and e-Learning
Version:	1
Approved By:	MIE Governing Body
Policy Approval Date:	January 2019
Date of Next Policy Review:	April 2023 (or as necessary)

MIE IT Information Security Policy

1. Context

Information is a critical asset of Marino Institute of Education, hereafter referred to as 'MIE'. Accurate, timely, relevant, and properly protected information is essential to the success of MIE's academic and administrative activities. MIE is committed to ensuring that all accesses to, uses of, and processing of MIE information are performed in a secure manner.

1.1. MIE is committed to adopting a security model in line with ISO27001 international best practice standards.

1.2. Technological Information Systems hereafter referred to as 'Information Systems' play a major role in supporting the day-to-day activities of MIE. These Information Systems include, but are not limited to, all Infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store Information owned by MIE.

1.3. The object of this Information Security Policy is to define the security controls necessary to safeguard MIE Information Systems and ensure the security confidentiality and integrity of the information held therein.

1.4. The Policy provides a framework in which security threats to MIE Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of Information security controls throughout MIE.

1.5. MIE recognises that failure to implement adequate Information security controls could potentially lead to:

i. Financial loss

ii. Irretrievable loss of Important MIE Data

iii. Damage to the reputation of the MIE

iv. Legal consequences.

1.6 Therefore, measures must be in place which will minimise the risk to MIE from unauthorised modification, destruction or disclosure of data, whether accidental or deliberate. This can be achieved only if all staff and students observe the highest standards of ethical, personal and professional conduct.

1.7 Effective security is achieved by working with a proper discipline, in compliance with legislation and MIE policies, and by adherence to approved Codes of Practice.

1.8 The Information Security Policy and supporting policies apply to all staff and students of MIE and all other users authorised by MIE.

1.9 The Information Security Policy and supporting policies do not form part of a formal contract of employment with the MIE, but it is a condition of employment that employees will abide by the regulations and policies made by MIE from time to time.

1.10 Likewise, the policies are an integral part of the MIE Staff & Students Code of Conduct for Use of IT Systems.

1.11 The Information Systems Security Policy and supporting policies relate to use of, but are not limited to:

v. All MIE networks, systems and services hosted therein

vi. All MIE-owned/leased/rented and on-loan facilities

vii. All private systems, owned/leased/rented/on-loan, when connected to the MIE network directly, or indirectly

viii. All MIE-owned/licensed data/programs, on MIE and on private systems

ix. All data/programs provided to the MIE by sponsors or external agencies, or licensed offices.

2. Policy Objectives

The objectives of the Information Systems Security Policy and supporting policies are to:

2.1 Ensure that information is created, used and maintained in a secure environment.

2.2 Ensure that all of MIE's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.

2.3 Ensure that all users are aware of and fully comply with the Policy Statement and the relevant supporting policies and procedures.

2.4 Ensure that all users are aware of and fully comply with the relevant Irish and European Community legislation.

2.5 Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.

2.6 Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

2.7 Ensure that all MIE owned assets have an identified owner/administrator.

3. IT Security Governance

Governance outline

3.1. Security of MIE's IT and data assets cannot be achieved without a coherent governance model that ensures that all IT systems in MIE are operated in accordance with approved policy and best practice.

3.2. The MIE security model seeks to clearly define who is authorised to operate key IT systems and services and how individuals and groups wishing to operate new systems or services are approved and subsequently governed.

4. MIE Data Network

4.1. This is the main MIE network serving the entire staff and student population. This network is operated by members of the IT Team and provides central services and support to all users.

4.2. The services of the main MIE network are available to all users including users who are also members of other autonomously managed networks hosted on MIE's network.

5. The Network Perimeter

5.1. Access through the network perimeter firewall is managed and operated by IT Team.

5.2. Individuals located in the main MIE network may make direct application for access through the firewall.

6. Communications

6.1 Good quality and frequent communications between all parties defined in this model are vital.

6.2 Communications by members of the IT Team are facilitated by a helpdesk which can be used by staff and students alike.

7. Heads of Function

7.1 Heads of Function are required to familiarise themselves with the policies.

7.2 Where a policy breach is highlighted, Heads of Function must co-operate in ensuring that appropriate action is taken. Heads of Function are obliged to ensure that all IT systems under their remit are formally administered either by an administrator appointed by the Head of an academic and administrative area or centrally by IT Team.

8. Autonomous Networks

Where an area operates an autonomous network with a connection to MIE Network such as a local database, then the respective Head of Function is required to ensure that their operations comply with the Information Security Policy.

9. The Information Security Officer or designate

The Information Security Officer, or their designate, is responsible for:

9.1. Advising the Governing Body[1], the MIE Heads of Function, Administrators and other appropriate persons on compliance with this policy and its associated supporting policies and procedures.

9.2. Reviewing and updating the Security policy and supporting policies and procedures.

9.3. The promotion of the policy throughout MIE.

9.4. Periodical assessments of security controls as outlined in the Security Policy and supporting policies and procedures.

9.5. Investigating Security Incidents as they arise.

9.6. Maintaining Records of Security Incidents.

i. These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed.

ii. The records will then be held in this anonymous format for a further two years for statistical purposes[2].

9.7. Reporting to the Governing Body[1], the MIE Heads of Function, Administrators and other appropriate persons on the status of security controls within the MIE.

10.The Director of IT & e-Learning

The Director of IT and e-Learning or their deputy is responsible for the management of MIE Network and for the provision of support and advice to all nominated individuals with responsibility for discharging these policies.

[1] See Code of Governance and Matters Reserved for the Governing Body of MIE

[2] See Data Protection Policy, Record Management Policy and MIE Records Retention Schedule

11.Information Systems Users

11.1. It is the responsibility of each individual Information Systems user to ensure their understanding of and compliance with this Policy and the associated Codes of Practice.

11.2. All individuals (staff and students) are responsible for the security of MIE Information Systems assigned to them.

i. This includes, but is not limited to, infrastructure, networks, hardware and software.

ii. Users must ensure that any access to these assets which they grant to others is for MIE use only, is not excessive and is maintained in an appropriate manner.

12. Purchasing, Commissioning, Developing an Information System

12.1. All individuals who purchase, commission or develop an Information System for MIE are obliged to ensure that this system conforms to necessary security standards as defined in this Information Security Policy and supporting policies.

12.2. Individuals intending to collect, store or distribute data via an Information System must ensure that they conform to MIE defined policies and all relevant legislation.

13.Third Parties & Licenced Offices

13.1 Before any third-party users are permitted access to MIE Information Systems, a written third-party agreement is required.

13.2 Prior to being allowed to work with MIE Information systems, satisfactory references from reliable sources should be obtained and verified for all third parties which includes, but is not limited to, administrative staff, software support companies, engineers, cleaners, contract and temporary appointments.

13.3 Data processing, service and maintenance contracts should contain an indemnity clause that offers cover in case of fraud or damage. Independent third-party review of the adequacy of and compliance with information system controls must be periodically obtained.

14. Reporting of Security Incidents

14.1 All suspected information security incidents must be reported as quickly as possible through the appropriate channels.

14.2 All MIE staff and students have a duty to report information security violations and problems to the Information Security Officer on a timely basis so that prompt remedial

action may be taken[3].

14.3 The Information Security Officer will be responsible for setting up an Incident Management Team to deal with all incidents.

14.4 Records describing all reported information security problems and violations will be created. These records will be encrypted and stored securely for six months after which time all information pertaining to individuals will be removed[4].

14.5 The records will be held in this anonymous format for a further two years for statistical purposes.

15. Security Controls

15.1. All MIE Information Systems are subject to the information security standards as outlined in this and related policy documents.

15.2. No exceptions are permitted unless it can be demonstrated that the costs of using a standard exceed the benefits, or that use of a standard will clearly impede MIE activities.

16. Compliance with Legislation

16.1 MIE has an obligation to abide by all Irish legislation and relevant legislation of the European Community.

16.2 The relevant acts which apply in Irish law to Information Systems Security include, but are not limited to:

i. The General Data Protection Regulation (GDPR) 2016/679
ii. European Communities (Data Protection) Regulations (2001)
iii. European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
iv. Criminal Damage Act (1991)
v. Child Trafficking and Pornography Act (1998)
vi. Intellectual Property Miscellaneous Provisions Act (1998)
vii. Copyright and Related Rights Act (2000)
viii. Health and Safety Act (1989)
ix. Non-Fatal Offences Against the Person Act (1997)

[3] See MIE Staff & Students Code of Conduct for Use of IT Systems and MIE Disciplinary Policy
[4] See Data Protection Policy, Record Management Policy and MIE Records Retention Schedule

x. Electronic Commerce Act (2000)

xi. Directive on Electronic Commerce (2000/31/EC)

xii. S.I. No. 68/2003 - European Communities (Directive 2000/31/EC) Regulations 2003.

16.3 The requirement for compliance devolves to all users as defined above, who may be held personally responsible for any breach of the legislation. Summaries of the legislation most relevant to MIE's IT policies may be found in the Guidelines accompanying the Policies.

16.4 Full texts of the most relevant legislation are available from the MIE Library, IT Services and associated website and the MIE Information Security Officer.

17. Breaches of Security

17.1. Monitoring

IT Services will monitor network activity, reports from the Computer Emergency Response Team (CERT) and other security agencies and take action/make recommendations consistent with maintaining the security of MIE information system.

17.2. Incident Reporting

Any individual suspecting that there has been, or is likely to be, a breach of information systems security should inform the Information Security Officer or the Director of IT and e-Learning immediately who will advise on what action should be taken.

17.3. Enforcement

i. The Director of IT and e-Learning or their delegated agent has the authority to invoke the appropriate MIE disciplinary procedures to protect MIE against breaches of security.

ii. In the event of a suspected or actual breach of security, the Director of IT and e-Learning, their delegated agent or the Information Security Officer may, after consultation with the relevant Administrator, make inaccessible/remove any unsafe user accounts, data and/or programs on the system from the network.

18. Legal Implications

18.1 Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the General Data Protection Regulation (GDPR) and could lead to civil or criminal proceedings and/or regulator

fines.

18.2 All staff and students are advised to familiarise themselves with and comply with this policy and with the MIE Data Protection Policy.

19. Disciplinary Procedures

19.1. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken[5].

19.2. Failure of a contractor to comply could lead to the cancellation of a contract.

20. Policy Awareness and Distribution

20.1. New Staff and Students

i. This Policy Statement will be available from IT Team on request.

ii. It will also be published on the IT web site and virtual learning environment.

iii. New staff and students will be notified of the relevant policy documents on commencement of employment or student registration.

20.2. Existing Staff

i. Existing staff and students of MIE, authorised third parties and contractors given access to the MIE network will be advised of the existence of this policy statement.

ii. They will also be advised of the availability of the associated policies and procedures which are published on the MIE website and virtual learning environment.

20.3. Updates

Updates to Policies and procedures will be made periodically and will be posted to the MIE web site and virtual learning environment.

21. Risk Assessment and Compliance

21.1 Risk assessments must be carried out periodically on the business value of the information users are handling and the information systems security controls currently in place.

21.2 This is to take into account changes to operating systems, business requirements, and MIE priorities, as well as relevant legislation and to revise their security arrangements accordingly.

[5] See Disciplinary Policy

22. Information Security Officer

The Information Security Officer will carry out risk assessments, review all risk assessments completed by other parties and highlight any measures needed to reduce risk in Information Security areas.

23. Internal Audit

23.1. The MIE Internal Auditor will periodically facilitate the assessment of risk management and compliance with the Information Security Policy.

23.2. Third-Party Audits will be carried out at intervals, as deemed necessary by the Internal Auditor and/or the Director of IT and e-Learning and/or Chief Financial Officer or their deputy.

24. Supporting Policies, Review Documentation and Guidance Notes

24.1. Supporting Policies amplifying this Policy Statement and Codes of Practice[6] associated with these policies are published in an accompanying document and are available on the IT Services web site or on request from IT Services.

24.2. Staff, students and any third parties authorised to access the MIE Network to use the systems and facilities as identified in this policy, are required to familiarise themselves with the policies and to work in accordance with them.

25. Responsibility

25.1 The Director of IT & e-Learning has responsibility for this Policy.

25.2 The Director of IT & e-Learning, with support from the Head of Department, is responsible for the implementation of this policy.

25.3 The Director of IT & e-Learning is responsible for technical service standards and management of the contract with our security suppliers.

[6] See MIE Staff & Students Code of Conduct for Use of IT Systems

26.Related Documents

26.1. MIE IT Acceptable Use Policy

26.2. Purchasing of Goods and Procurement of Services

26.3. Accessible Information Policy

26.4. Blended and Online Learning Quality Assurance Policy

26.5. Disciplinary Policy

26.6. MIE Virtual Learning Environment Policy

26.7. MIE Staff & Students Code of Conduct for Use of IT Systems

26.8. Data Protection Policy

26.9. Code of Governance

26.10. Matters Reserved for the Governing Body of MIE

26.11. Record Management Policy

26.12. MIE Records Retention Schedule