Information Management Security Policy and Protocols

Document Type	Policy
Administering Entity	Board of Directors
Latest Approval/Amendment Date	30 October 2020
Last Approval/Amendment Date	-
Approval Authority	Board of Directors
Indicative time of Review	30 October 2023

1. Purpose

The purpose of this Policy is to outline the obligations on staff, students and authorised third parties of the Analytics Institute of Australia (AIA) who access and use the AIA's Information Management systems to maintain security of the network and data.

2. Scope

a. This Policy applies to all AIA staff and students and other authorised users of AIA Information Management Systems. It covers assets including, but not limited to:

- Information assets (e.g. databases, files, electronic documents)
- Software assets (e.g. applications, software tools, licences); and
- Physical assets (e.g. computers, servers, network infrastructure, information storage media, printers, communications equipment, AV equipment, projectors, telephones and facilities)

b. The Policy applies to security breaches or any risk of threats arising from:

- On-campus devices not approved for network connection
- On-campus networks not installed or approved AIA IT management
- Off-campus networks and devices

insofar as action is required to mitigate, remove or neutralize any apparent risk or threat to IT security.

3. Principle

All staff, students and users who are given access to AIA information systems must agree to abide by the AIA's information security and privacy policies.

General IT Security

a. At any point, on or off campus, that AIA IT resources are being used, all relevant policies will be applicable.

b. AIA retains the right to monitor and control ITM systems and their content, including network and system activity, in accordance with staff and student Codes of Conduct and the AIA Privacy Policy and in a manner which respects the rights and legitimate interests of those concerned.

c. The authority to inspect machines, servers and files resides with the Chief Operating Officer (COO). Disclosure to an external organisation will only be considered on production of a legal authority.

d. Systems that are deemed to pose a threat to the AIA network may be disconnected from the network, without prior notice, by IT Support, under authority and instruction of the COO.

e. The AIA reserves the right to suspend or terminate access to a user account in cases of suspected security breaches, inappropriate or illegal activity, or unauthorised access. This includes staff, student, and affiliate accounts.

f. Security incidents will be handled in accordance with the AIA Business Continuity and Critical Incident plans.

g. All major systems and information assets will be accounted for by IT support and Area Managers will be responsible for the implementation and management of this policy in relation to those assets.

h. All AIA managed systems will be maintained to a base line of security through best practice security controls such as regular patching and centralised management.

i. Network services and software applications which require higher levels of security will only be accessible remotely via the AIA's Virtual Private Network (VPN).

j. Staff, students and authorised third parties who use public access or other non-AIA IT services to access AIA resources are obliged to respect the AIA security policies as well as the relevant security policies of the remote service.

k. To ensure that no private or confidential information is exposed, any user accessing a secure system remotely should do so only on trusted networks.

l. AIA-owned data or information may not be stored using public storage services, i.e. Dropbox or similar, except under an AIA approved contractual arrangement.

m. Any data breaches, or suspected data breaches, must be reported to IT Support immediately upon discovery.

n. Access to AIA's network services by students will be removed from the first day of the study period if the student fails to enroll or from the date of graduation, whichever comes first

o. Access to the AIA's network services by staff will be removed at close of business, on the staff member's termination date.

User Account and Password

a. Users must activate a password protection method to secure their workstation or devices with AIA network access or content. All devices should be locked prior to leaving unattended.

b. All mobile devices, including phones, tablets and laptops, that are used to access or store AIA data or information should be password or passcode protected. This applies whether the device is an AIA asset or a personal device.

c. Each authorised user will be issued with a user ID

d. All general access to AIA corporate systems should be configured to utilise the authorised user's account and associated password. Exceptions to this rule are:

- Systems which require an additional level of security which warrants a separate password due to elevated levels of access - this requires approval by the COO.
- Systems that that are not under the control of AIA and which are not operating under a contract or agreement with the AIA. Such systems must NOT use the authorised user account and password.
- Systems that do not store or transmit the password in encrypted format. Such systems must NOT use the authorised user account and password.

e. The onus of protecting their password is on each individual. The password must not be used on other systems, shared or disclosed with anyone- including assistants or family.

f. The possession of an account and a password that enables access to read or update particular information does not constitute the authority to do so. Such authority must be explicitly granted by COO. It is the responsibility of COO to audit key corporate system privileges and ensure they are commensurate with current staff roles.

g. It is recommended that user-level passwords be changed at least every six months. User-level passwords must be changed if they do not meet the AIA's complexity requirements or are known to other individuals.

h. Passwords for privileged accounts must be changed at intervals as follows:

- Executive Leadership Group members: every 8 weeks in addition to the requirements for user-level passwords.
- System-level passwords (e.g. administrator): as per user-level passwords and otherwise changed every 6 months automatically where possible. Where auto changes are not supported, system-level passwords must be changed every time a staff member with access to the password leaves the AIA.

i. All passwords must:

- Contain eight characters or more
- Contain lower-case letters, upper-case letters, numbers and nonalphanumeric characters

j. All system-level passwords (e.g.,administrator) must be stored in a secure place designated by IT Support.

Special Case Data Access

a. Access to a current staff member's electronic data, which includes email, and documents stored centrally (e.g. H: drive) or locally (e.g. C: drive), is only permitted if accompanied by a business case, approved by the COO.

b. Where reasonable grounds exist to justify accessing a former staff member's email or electronic files, access may be provided to the supervisor or other nominated staff as approved by the COO after consideration of a business case.

Privately Owned Devices

a. Privately owned devices may be connected to the AIA network (wired or wireless) provided that these meet basic levels of security as determined by the AIA.

b. AIA reserves the right to inspect all privately owned devices which are connected to the AIA network to investigate suspected security breaches, inappropriate or illegal activity, or unauthorised access.

c. Privately owned devices that are deemed to pose a threat to the AIA network may be disconnected from the network without prior notice, by IT Support, under the authorisation of the COO.

d. AIA accepts no responsibility for any loss or damage to either the physical device or data contained within it as a result of bringing the device onto the AIA campus, connecting it to the AIA network and/or using it for AIA business.

e. AIA accepts no responsibility for the support and maintenance of privately owned devices whether or not they are used for AIA business. This includes privately owned data storage media connected to staff or student workstations.

f. AIA owned data or information must not be stored on privately owned equipment.

Third Party Contract and Access Security

a. Contractors, outsourced providers, service suppliers and other third party providers may be involved in AIA operations. This may include, but is not limited to, the following circumstances:

- third party system design, development or operation of AIA services;
- access granted from remote locations where computer and network facilities may not be under the control of the AIA; or
- when authorised third party providers are given access to information or information systems

b. All third-party providers who require access to AIA information systems must agree to comply with all relevant policies at the time of contract signing.

c. Due to the confidentiality, sensitivity or value of the information that may be accessed, AIA may require third party providers to sign a confidentiality agreement to protect its information assets.

d. All contracts with third party providers for the supply of services to AIA must be monitored and reviewed to ensure that information security requirements are being satisfied.

e. Authorised third party providers must be given minimum access privileges to meet their contractual requirements. They are not permitted to copy or store any AIA information for any reason other than that required to complete the terms of their contract.

f. All third-party providers must report any instance, including physical, of unauthorised access, transmission, or loss (or suspected loss) of AIA data by a third party. In addition, third party providers must report IT security incidents that may impact systems connected to AIA systems.

IT Physical Security

a. IT assets are generally associated with the physical devices on which information resides and includes, but is not limited to, workstations, servers and the physical network infrastructure

b. Physical access controls around computing locations are to be applied in a manner that reflects the business value and criticality of IT services hosted in the location and the value of the data stored

c. No computer equipment is to be removed from any office, work area or computer laboratory unless specific authorisation has been received from IT Support.

d. Persons who are issued with portable AIA IT assets, such as laptops, must agree to personal responsibility of the equipment. When not in use, all portable AIA IT assets must be secured

e. Computer laboratories and other locations that house ITM assets must employ physical access controls such as electronic or physical locks.

4. Responsibilities

The Chief Operating Officer is responsible for maintenance and implementation of this policy

5. Legislation and Associated Documents

The following legislation is relevant to this Policy:

- Privacy and Data Protection Act 2014. (Vic)
- Copyright Act 1968 (Cth),
- The Freedom of Information Act 1982 (Cth)
- Crimes Act 1914 (Cth).

The following Standards in the Higher Education Standards Framework are relevant to this Policy: 3.3.2, 7.3.3

6. Supporting Information

The following AIA policies and procedures are relevant to this Policy

- IT Acceptable Usage Policy
- Records Management Policy and Procedures
- Staff Code of Conduct Policy
- Student Code of Conduct Policy
- Student Performance Data Policy and Procedures
- Graduation and Certification Policy
- Business Continuity Plan
- Critical Incident Policy

Version history

Version	Approved by	Approval Date	Details
1.0	Board of Directors	30/10/2020	

Document owner: Board of Directors