Information and Communications Technology Security Policy

Purpose/objective

This Policy provides the framework that ensures appropriate controls are in place to protect AAHE's enterprise information and communications technology (ICT). The Information and Communications Technology Security Procedure explains how this Policy is implemented.

ICT and data management underpins AAHE's operations and must therefore be an integral part of AAHE's management and business processes. The security of AAHE's ICT and data is essential in order to maintain business performance standards and continuity, legal compliance and adherence to AAHE's own policies and procedures.

There are many policies and related documents that should be read in conjunction with this Policy. These are listed below under **Related Documents and Legislation**.

Scope

This Policy and Procedure applies to:

- all AAHE staff and students, contractors, visitors and any other parties that have access to AAHE's information and communications technology systems, resources and networks
- ICT resources owned, leased or operated by AAHE or third parties on behalf of AAHE.

Definitions

Terms used in this document are defined in the AAHE Glossary.

Policy

1. Key principles

1.1 AAHE is committed to providing its students with the latest ICT systems and resources that support their learning and their engagement with fellow students, staff and with AAHE's administrative processes.

1.2 AAHE will provide its students, staff and affiliates with ICT systems and resources that are fit for purpose, accessible, reliable and promote innovation and creativity.

1.3 AAHE's ICT systems and resources are critical to its smooth operation and must therefore be protected against accidental or malicious misapplication, unauthorised access or disclosure, modification, corruption, or destruction.

1.4 ICT systems and resources must be adequately managed and supported so that they are physically, operationally and technically safeguarded without imposing unnecessary restrictions on the conduct of AAHE's business.

1.5 All students shall be provided equitable access to ICT resources in accordance with AAHE's Equity and Diversity Policy and Procedure.

1.6 AAHE's ICT systems and resources must comply with the relevant standards in the Higher Education Standards Framework (Threshold Standards) 2021 and relevant legislation.

2. ICT Security

2.1 ICT systems and resources must be appropriately managed and secured with controls to preserve:

- ***Confidentiality*** - information is protected from unauthorised disclosure
- ***Integrity*** - information is accurate, current and has not been altered without authorisation
- ***Availability*** - critical information can be readily accessed when required; and
- ***Accountability*** - individuals or parties are responsible for their actions when using AAHE's ICT systems and resources.

2.2 AAHE's ICT systems must be secured by appropriate access controls and authentication mechanisms.

2.3 No individual or party shall attempt to circumvent the security mechanisms of any AAHE computer system or network without authorisation from the COO.

2.4 AAHE's ICT systems must be monitored with effective malicious software management systems, and the Managed Operating Environment (MOE) must be regularly updated with the latest software versions and security patches.

2.5 Regular vulnerability assessments will be undertaken across ICT systems using appropriate tools. Where threats and vulnerabilities are identified, the risk will be evaluated and managed, and, if required, AAHE's Risk Register will be updated.

2.6 Critical ICT systems must have effective backup procedures and disaster recovery plans that are documented and tested periodically.

2.7 Devices connected to AAHE's network must be secure and comply with network security provisions.

2.8 Use of all ICT systems must comply with the Acceptable Use of ICT Policy.

2.9 IT assets must be recorded on an asset register for the purpose of identification, audit and investigation.

2.10 Internally and externally hosted data centres/server rooms must be physically robust and reasonably protected against flooding, fire, vibration, dust and other natural elements that could present a threat to their integrity and security.

2.11 Data centres/server rooms must employ mechanisms to control air temperature and humidity.

2.12 Combustible material must not be stored in data centres/server rooms.

2.13 Critical ICT systems must have a back-up power source able to provide an uninterrupted power supply in the event of a mains power failure.

2.14 Access to data centres/server rooms is restricted to authorised staff only. They must be adequately secured and protected by an appropriate access control system and surveillance systems.

2.15 All of AAHE's ICT systems and the data and information they contain must be adequately protected against cyber attacks.

3. User Access Controls

3.1 Staff members and students will be issued with unique usernames and passwords upon formal commencement with AAHE.

3.2 Users are responsible for keeping their User ID and Password protected and are prohibited from sharing or disclosing their account details.

3.3 Business critical and highly confidential information systems and networks should require multifactor authentication.

4. External Service Providers

4.1 All outsourcing and hosting contracts between external providers and AAHE for services and equipment must be in line with the ICT Provisioning Policy and Procedure.

4.2 The IT/LMS Officer will monitor and review external provider's services to ensure appropriate security controls are implemented and maintained.

4.3 The responsibility for security of equipment deployed by external service providers and the data contained within such equipment must be clarified in the contract with the services provider and include all documentation of security contacts and escalation procedures.

Related documents and relevant legislation

Acceptable Use of Information and Communications Technology Policy
Business Continuity Management Policy
Cyber Incident Response Plan
Delegation of Authority Policy
Equity and Diversity Policy
Higher Education Standards Framework (Threshold Standards) 2021
Information and Communications Technology Provisioning Policy
Information Management and Security Policy
Privacy Policy
Quality Assurance Policy
Records Management Policy
Resources and Infrastructure Plan
Risk Management Policy, Risk Register, Risk Measurement
Student Code of Conduct
Staff Code of Conduct
Teaching and Learning Plan

Document information

Document owner: Board of Directors

Version	Approved by	Approved on	Implementation date	Changes made
1	Board of Directors	16/9/21	1/10/23	

Information and Communications Technology Security Procedure

The Information and Communications Technology Security Policy draws on a number of AAHE policies, procedures and plans for its effective implementation. The relevant procedures can be found in the following documents:

- ICT Provisioning Policy and Procedure
- Acceptable Use of ICT Policy and Procedure
- Cyber Incident Response Plan
- Student Communications and Information Policy and Procedure
- Privacy Policy and Procedure
- Critical Incident Policy and Procedure
- Records Management Policy and Procedure.

Roles and responsibilities

RESPONSIBILITIES
Executive Management Committee
• executive oversight, decision-making and coordination in relation to AAHE business, including the implementation of AAHE's ICT related policies, procedures and plans • performing the role of Critical Incident Response Team for ICT critical incidents and security breaches, as defined in the AAHE Critical Incident Policy and the Cyber Incident Response Plan
Audit, Risk and Finance Committee
• monitoring ICT security risks and controls by reviewing the outcomes of risk management processes and monitoring emerging risks • reporting to the Board of Directors on risks pertaining to ICT security capability and controls • overseeing the risk management plan and framework and ensuring that it effectively facilitates the identification, monitoring, assessment and mitigation of key higher level ICT security risks across of AAHE and its operations • ensuring that AAHE is supported with a contemporary quality and compliance audit program that provides appropriate depth and breadth of coverage in terms of ICT • reviewing internal and external ICT security audit reports to ensure that recommendations and agreed actions are promptly enacted • facilitating the conduct of special ICT security investigations initiated by the committee or requested by the Board of Directors as required • overseeing the effectiveness of AAHE's ICT security compliance framework
Chief Operating Officer
• Overall management and implementation of the AAHE Business Continuity Policy, ICT Provisioning Policy, ICT Security Policy and related policies and plans • Ensuring the effectiveness of ICT security measures and control processes, including the implementation, review and refinement of the Cyber Incident Response Plan

- Chairing the Cybersecurity Defence Team meetings (refer to Cyber Incident Response Plan)
- Ensuring the effectiveness of disaster recovery plans through a regular program of ICT vulnerability testing to be undertaken by the IT/LMS Officer
- Approving the isolation or disconnection from the network of any equipment or ICT facility that poses a severe and unacceptable risk
- Reporting to the Audit, Risk and Finance Committee, Executive Management Committee and the Board of Directors on risks pertaining to ICT security and information management
- Ensuring all authorised users comply with the policies and procedures around 'acceptable use' of AAHE's ICT systems and resources
- Ensuring all staff undertake staff induction and annual compliance training modules in ICT Security and Information Management (refer to Staff Training Program)
- Implementing disciplinary action for inappropriate use of ICT systems and resources by staff
- Representing AAHE with external bodies, including law enforcement, on ICT security matters

IT/LMS Officer

- Ensuring that there is broad awareness of ICT security across AAHE and that appropriate resources including information and advice are available as required on ICT security matters
- Investigating any reported ICT security incidents or risks and respond appropriately
- Providing authenticated access to ICT systems and resources to authorised users within AAHE
- Undertaking vulnerability risk assessments of ICT systems to determine the probability and impact of security failures, and recommend appropriate mitigation strategies
- Maintaining an up-to-date Managed Operating Environment (MOE) and ensuring staff have access to a published list of the approved MOE hardware and software
- Assessing all non-MOE approved hardware and software requests and investigating their suitability for inclusion in the MOE, viability as a standalone system, compliance with relevant policies and total cost of ownership
- Managing all procurement of ICT hardware, software and cloud services
- Endorsing and managing all software and hardware that is installed on the AAHE network
- Maintaining an up-to-date register of all ICT hardware and software, where they are located and to whom they are assigned
- Maintaining systems logs including access, activity and performance logs for auditing purposes and according to regulatory and business needs
- Providing regular reports to the COO on ICT activity, performance and security matters as required

Registrar
• Authorising legal access to users' private information held or stored by AAHE in order to investigate suspected breaches of AAHE policies and procedures, or as required by law. • Ensuring that all students are made fully aware of the ICT Security Policy, Acceptable Use of ICT Policy and related policies • Implementing disciplinary action for inappropriate use of ICT systems and resources by students
Quality Assurance Manager
• Conducting internal audits of ICT and security related policies, procedures and plans and providing independent assessment of their adequacy • Ensuring AAHE compliance with the *Higher Education Standards Framework* and relevant regulations and legislation as they relate to ICT and information management security • Conducting ongoing ICT and information management security risk assessments against the AAHE Risk Matrix and maintaining the Risk Register • Participating as a member of the Cybersecurity Defence Team and undertaking regular review and improvement of the Cyber Incident Response Plan • Managing post incident reviews after each critical incident response and facilitating the implementation of any learnings as improvements to policies, procedures, plans, training programs etc • Developing a quality assurance training program including ICT security and information management for incorporation into staff induction and annual compliance training modules
Managers and Heads of Department
• Ensuring that all information in their area is managed and conforms to relevant AAHE policies and procedures, and legislative requirements • Making themselves familiar with risk assessments for the ICT systems used within their area of responsibility, and ensuring that relevant risk mitigation measures are implemented as appropriate • Ensuring that all staff, contractors and visitors are made fully aware of the ICT security and related policies, and are given appropriate support and resources to comply • Ensuring that all staff under their supervision are properly inducted and are aware of their responsibilities with respect to ICT and information management policies, procedures and user guidelines when they commence employment with AAHE • Ensuring all staff under their supervision complete the annual compliance training modules in ICT Security and Information Management
Users of ICT systems and resources
• Using ICT systems and resources according to AAHE policies, procedures and guidelines at all times

- Being aware of the security requirements of the ICT systems and resources that they use, and taking every precaution to safeguard their access to these systems against unauthorised use
- Engaging the IT/LMS Officer for all procurement of ICT hardware, software and cloud services
- Ensuring that the IT/LMS Officer endorses and manages all software and hardware that is installed on the AAHE network
- Keeping their User IDs and passwords secure and private
- Immediately reporting any known or suspected security incidents and breaches
- Not communicating the ICT security risks, controls, events and incidents outside AAHE except where required or authorised to do so by law.

Document information

Document owner: Chief Operating Officer

Version	Approved by	Approved on	Implementation date	Changes made
1	Board of Directors	16/9/21	1/10/23	