AECC University College

IT Security & Password Policy

1. Introduction

1.1. This policy defines a framework by which the AECC's computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

1.2. The University is required to ensure that its information assets are adequately protected by passwords and other appropriate means of security in order to fulfil its legal and legislative duties. All users must take all necessary steps to protect and maintain the security of all University hardware, systems, software and data.

1.3. Technical controls will be enforced where possible, but users are also responsible for adhering to this policy.

2. Scope

2.1. Applies to all staff, students and guests (including volunteers, casual and fellows) requiring access to University IT systems.

3. Key Principles

3.1. All University computer systems, environments and information contained within them must be protected against unauthorised access.

3.2. All use of all IT facilities must comply with the IT Acceptable Use Policy

3.3. Information kept within these systems will be managed securely, to comply with relevant data protection laws and to satisfy the institution's expectations that such assets will be managed in a professional, safe and dependable manner.

3.4. All members of AECC UC should familiarise themselves with this policy, to adhere to it and comply with its requirements.

3.5. All regulatory and legislative requirements regarding computer security and IT based information confidentiality and integrity will be addressed by the University.

3.6. All breaches of security will be reported to and initially investigated by the IT Team, who will involve the DPO (Data Protection Officer) where appropriate.

4. Responsibilities

4.1. The IT Team employ multi-layered security controls to protect the network infrastructure and the data contained within. This policy dictates the minimum expectations of all users to maintain security of accounts and computing facilities.

4.2. All users with an institution provided email address are expected to attend and complete any mandatory Cyber Security and Data Protection Training and maintain cyber awareness by paying attention to relevant emails and other guidance that may be issued by the institution, particularly in response to prevalent threats.

4.3. Heads of Department and line managers have a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of responsibility.

4.4. Systems Owners are responsible for ensuring that appropriate technical controls are enforced within systems where available including but not limited to: enforcing MFA where available Systems owners must also ensure that third party suppliers hold up to date security assurances and certifications such as Cyber Essentials and ISO27001.

4.5. All users have a responsibility to report promptly (to the IT Team) any incidents which may have an IT security implication for the University.

5. The Computing Environment

5.1. The IT Team manages, maintains and operates a range of central servers, systems, network switches, backup systems, and the overall network infrastructure interconnecting these systems.

5.2. The computing environment is defined as all central computing resources and network infrastructure managed and overseen by the IT Team and all computing devices that can physically connect to it, and have been authorised to connect to this environment. All are covered by this policy, including computing hardware and software, any AECC UC related data residing on these machines or accessible from these machines within the campus network environment and any portable media such as CDs, DVDs, portable storage devices and backup tapes.

5.3. All temporary and permanent connections to the AECC network including wireless networks and VPN connections are similarly subject to the conditions of this policy.

5.4. Computing resources not owned by the University may only be connected to the wireless networks.

5.5. The IT Team reserves the right to monitor, log, collect and analyse the content of all transmissions on networks maintained by the IT Team at any time deemed necessary for performance, fault diagnostic and policy compliance purposes.

6. Passwords

6.1. Passwords are a key part of the University's Strategy to protect all institutional IT resources from unauthorised access. The security of any account is completely dependent on the security of the password.

6.2. The following password requirements will be enforced by the IT Team for Active Directory and Microsoft 365 accounts and should be enforced by Systems Owners of systems outside of the IT Team's control where supported by the system. For their own protection, all users are also encouraged to follow these password rules for any personal accounts.

6.3. All passwords should be suitably complex and difficult for others to guess. The IT Team can provide guidance as to how to set a good password.

6.4. Passwords must meet the following requirements:

6.4.1. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters

6.4.2. Be at least eight characters in length (longer passwords or passphrases are strongly encouraged. Current best practice recommendations are to use three random words)

6.4.3. Contain characters from three of the following four categories:

6.4.3.1. English uppercase characters (A through Z)

6.4.3.2. English lowercase characters (a through z)

6.4.3.3. Base 10 digits (0 through 9)

6.4.3.4. Non-alphabetic characters (for example, !, $, #, %)

6.5. Complexity requirements are enforced when passwords are changed or created.

6.6. A password history will be retained to disallow a previous password to be reused.
6.7. Repeated incorrect password attempts will result in the account being locked out.
6.8. In addition to meeting those requirements, common sense should be used when choosing passwords. Avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective.
6.9. Personal information should not be used as a password hint, as this weakens the security of the account.
6.10. All users must choose unique passwords for all of their AECC UC accounts, and must not re-use a password that they are already using for a personal account.
6.11. Users with privileged or administrative accounts must use unique passwords for each different account.
6.12. Users must not share their passwords with anyone else in the University, including co-workers and managers, unless authorised to do so by the IT Team. This includes during periods of absence when mailbox delegate mailbox access for instance would be appropriate. If there is a legimate business need for a shared login, please refer to the IT User Access Policy.
6.13. Users are strictly prohibited from sharing the password of their account with anyone outside of the University including third party software suppliers.
6.14. Users must not write down their passwords and keep them at their desk. Memorable passwords must be chosen.
6.15. ‘Remember password’ features should not be used.
6.16. Password managers may be used to securely store a password database. Please consult with the IT team to confirm current supported options.
6.17. Any default or initial passwords set for new accounts should be changed immediately.
6.18. Users must notify the IT Team and change their password immediately if they have any reason to believe a password may have been revealed to another user, or otherwise compromised.
6.19. Passwords will be changed without notice in response to a security incident or where suspicious activity has been detected through monitoring.
6.20. All users should pay attention to current Cyber Security advice and training provided by the University to avoid being victim to phishing and other similar attacks.

7. Physical Security

7.1. Servers and networking equipment are housed in secure data centres with protected power arrangements and climate-controlled environments.
7.2. Back up tapes and media are stored in a secure safe with controlled access.
7.3. Any computer equipment in general office environments should be secured behind locked doors and workstations must always be locked when left unattended.
7.4. All desktop computers and similar IT equipment within public areas must be protected by appropriate physical lock mechanisms to prevent the computer and its components from theft.
7.5. Users must ensure that workstations are locked when left unattended.
7.6. All users must ensure they logout of computers and resources at the end of each session. This extends to logging out of individual websites as otherwise server sessions will remain open and could be subject to compromise.
7.7. Any portable devices supplied by the University must be encrypted.

7.8. Any unattended portable equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they should be hidden from view.

7.9. Any use of personal devices to access or store University data must be in accordance with the Bring Your Own Device (BYOD) Policy and Data Protection Policy.

7.10. Under no circumstances should any devices be connected to University networks without prior consultation with the Head of IT. Unauthorised devices will be removed and blocked. (This does not extend to the wireless networks).

7.11. The IT Team manages and maintains an audit of all institutional IT equipment and must be made aware of any new equipment and consulted with prior any purchases.

8. Data Security

8.1. AECC University holds a variety of sensitive data including personal Student and Staff information. Users must treat all data and information with appropriate care and may be held accountable for any inappropriate mismanagement or loss. Access to systems and data will be allocated as defined in the IT User Access Policy.

8.2. The University provides both secure network storage that is regularly backed up and secure Microsoft 365 storage. It is the user's responsibility to store all University data on the provided secure areas.

8.3. Sensitive information such as student, staff and patient personal identifiable information should never leave secure University storage facilities, and must never be stored or transmitted using unsupported services (i.e. Dropbox or Google Drive). If such an event is deemed as essential, IT staff must first be consulted and can advise on appropriate encryption methods and other safe guards. Failure to do so could constitute a serious breach of this policy and could also lead to breaches of Data Protection and/or GDPR which can result in significant financial penalties. Also refer to the University Data Classifications and guidance.

8.4. Removable media such as USB drives and CDs or DVDs must not be used without prior agreement with the Head of IT. Any specific uses must be logged by the IT Team as a mitigation.

8.5. Multifactor authentication (MFA) will be enforced where it is supported by a system.

9. Loss of Theft of Confidential Information

9.1. All incidences of loss or theft of confidential information should be reported so that they may be investigated. Where a breach relating to Data Protection or GDPR is suspected, the DPO will be consulted and the Data Protection Data Breach process will be followed. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information either inside or outside the University.

9.2. A security incident is any event that has resulted or could result in:

- 9.2.1. The disclosure of confidential information to any unauthorised person.
- 9.2.2. The integrity of the system or data being put at risk.
- 9.2.3. The availability of the system or information being put at risk.
- 9.2.4. Adverse impact, for example:
  - 9.2.4.1. Negative impact on the reputation of the University.
  - 9.2.4.2. Threat to personal safety or privacy.
  - 9.2.4.3. Legal obligation or penalty.
  - 9.2.4.4. Financial loss or disruption of activities.

9.3. All incidents must be reported to your immediate line manager and to the Head of IT. A written report should be submitted containing the following information:
  9.3.1. Details of the incident
  9.3.2. Date of discovery of the incident
  9.3.3. Place of the incident
  9.3.4. Who discovered the incident
  9.3.5. Category/classification of the incident
  9.3.6. Any action already taken if risk to organisation e.g. report to the police

9.4. In the case of a serious potential breach, the Head of IT, will instigate an investigation into the incident and will determine whether it should to be reported to any regulatory bodies or other third parties, e.g. insurers. The Head of IT will retain a central register of all such incidents occurring within the University.

9.5. The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform your line manager who will then decide whether a report should be made.

9.6. Examples of breach of security:
  9.6.1. Loss of computer equipment due to crime of carelessness.
  9.6.2. Loss of portable media devices, e.g. memory sticks etc.
  9.6.3. Accessing any part of any system using someone else's password.
  9.6.4. Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists.

9.7. Examples of a breach of confidentiality:
  9.7.1. Finding confidential/personal information either in hard copy or on a portable media device outside University premises or in any of the University's common areas.
  9.7.2. Finding any records about a staff member, student, or applicant in any location outside the University's premises.
  9.7.3. Passing information to unauthorised people either verbally, written or electronically.

10. Supporting Policies

10.1. IT Acceptable Use Policy
10.2. Bring Your Own Device Policy
10.3. IT User Access Policy
10.4. Data Protection Policy
10.5. Patch Management Policy

11. Policy Review and Maintenance

11.1. This policy will be reviewed annually.

Version:	1.4
Ratified by:	SMG
Originator / Author:	Head of IT
Reference source:	HE Exemplars
Date approved:	11th July 2023
Effective from:	11th July 2023
Review date:	July 2024
Target:	AECC University College Staff, Students and guests requiring IT access
Equality Impact:	No direct impact