Policy: Information Technology (IT) Policies

Policy Title	Information Technology Policies
Policy ID	2024.-v2-PTR_Po
Effective Date	June 2024
Responsible Office	Vice President for Administrative Affairs
Responsible Executive(s)	IT Office

Rules of Use

Access to AUM computing resources is a privilege granted with the presumption that every member of the AUM community will exercise it responsibly.

The use of AUM computing resources follows these priorities:

High: All educational, research and administrative purposes of AUM.

Low: Other uses indirectly related to university purposes that have an educational or research benefit, including news reading, Web browsing, chat sessions and personal communications.

Forbidden: Engaging in commercial activity not sanctioned by AUM authorities; intentionally denying or interfering with any network resources, including spamming, jamming and crashing any computer; using or accessing any AUM computing resource, or reading or modifying files, without proper authorization; using the technology to in any way misrepresent or impersonate someone else; sending chain emails; violating Maltese and international laws or AUM policies.

In making use of AUM's computing resources and network, users agree to:

Respect the privacy of other users.

Respect the desire for privacy, and refrain from inspecting users' files, except in certain well- defined cases. IT Administrators or Network Administrators, authorized by the IT Committee, who carry out standard administrative practices, such as backing up files, cleaning up trash or temporary files, or searching for rogue programs, are not considered to be violating privacy.

The following actions are prohibited:

- Accessing the contents of files of another user without explicit authorization from that user.
- Intercepting or monitoring any network communications not explicitly meant for you.

- Use of the systems to transmit personal or private information about individuals unless you have explicit authorization from the individuals affected. Distributing such information without permission from those individuals is also not permitted and possibly violate privacy laws. Creating or installing programs that secretly collect information about users. Gathering information on other users through software installed on any AUM computing resources.

2. Not impersonate any other person.

   Using AUM computing resources to impersonate someone else is not permitted. Using someone else's account without their permission, may be an act of fraud: especially since the account owner's name will be attached to the transactions performed. Anyone using someone else's account must clearly identify him/herself to recipients. Sending anonymous mail or postings is discouraged; however, if felt necessary or appropriate, it is normal etiquette to indicate that the message is anonymous or is signed by a pseudonym.

3. Not use any University computer or its network to violate any Maltese laws or AUM policies.

Examples are given below to avoid inadvertent violations. This list is not comprehensive. In case of doubt, the IT Committee should be contacted for clarifications.

- The AUM network must not be extended without explicit permission from the IT Department.
- Unauthorized use of routers, switches, modems and other devices can impact the security and stability of the network.
- AUM computing resources must not be used to attack computers, accounts, or other users by launching viruses, worms, Trojan horses, or carrying out other attacks on computers on AUM premises or elsewhere.
- Unauthorized vulnerability scans on systems must not be performed; such scanning is considered to be a hostile act.
- AUM computing resources must not be used to harass or threaten others.
- AUM computing resources must not be used to transmit fraudulent messages.
- AUM computing resources must not be used to transmit, store, display, download, print or intentionally receive obscene material, or to distribute pornographic material.
- All users of AUM wifi services are subject to Maltese and international laws.

Only equipment or accessories issued to faculty or staff personally by the IT staff may be removed from campus and only if permission has been granted by AUM leadership. For each instance, faculty or staff members must apply in writing to the IT Department in advance to take computer accessories, cameras, laptops, hardware and the like belonging to AUM out of the country. It is the responsibility of the person authorized to take the equipment off campus to secure the computer against theft or illegal access and to return the equipment undamaged

IT Security:

Users requesting access to AUM computing resources will be required to sign a statement on the appropriate user account request form indicating that they have read, understood, and agreed to abide by these guidelines.

Improperly secured wireless access points can compromise the security and performance of the AUM network, and provide easy access for intruders to steal passwords, destroy data and use University network and internet resources for unauthorized purposes. Any department that deploys wireless networking devices must, at a minimum, follow basic security practices.

Private access points for departments, i.e. other than public access points deployed by the IT staff, should be configured to disable 'Broadcast SSID' if this function is supported on the equipment. This requirement is needed to prevent interference with public access points deployed at AUM. All devices using wireless access points must have updated antivirus software.

In order to obtain access to AUM computing resources, users must bring any devices to the IT department for registration prior to it being connected to the AUM network. Users (faculty, staff, & student) must not share their passwords with anyone else nor allow anyone else to access the network using their account. Members of the AUM community must change their password if they believe that their username and password have been compromised and/or used without their permission.

Any wireless network that poses a threat or violates accepted practices may be disconnected from the AUM backbone network. If a serious security breach is in process, the LAN may be disconnected. It is the responsibility of the students, faculty, and staff to be knowledgeable regarding the provisions of these policies.

Network Security:

All network components should be managed and used in a secure way. Failure to follow proper security protocols may lead to disciplinary and/or legal proceedings. Network security includes the following:

a. Wi-Fi:
   - Personal devices and visitors may access internet during their visit to AUM by using AUM Guest wireless SSID and password. They can acquire internet access by asking for credentials from IT representatives.
   - Wi-Fi passwords should not be shared with people outside AUM. Passwords must be changed at the end of every three-month period.

b. Internet:
   - Access to AUM's internet is granted for business (and occasional personal) use only. The portal will give the users access to the internet by authenticating with active directory username and password.
   - Prohibited websites (P2P, Spams, Pornographic sites, and any or all the sites creating security risks), as well as individual devices which may cause potential security vulnerability and holes will be blocked.

c. Network devices and passwords:
   - AUM IT staff are responsible for securing administrator passwords for these devices. This information must not be shared with third parties.

- If a vendor needs to access to one of those network devices for troubleshooting the AUM IT staff will manage the temporary access as well as ensuring closure of the access point afterwards.

d. CCTV:

IP cameras are installed on each floor to provide a safe learning environment and monitor any misconduct or improper behaviors. Users are not allowed to remove or disconnect the cables connected to cameras or disable the cameras in any way.

Anti-virus software:

IT staff are responsible for installing anti-virus software on all computers owned by AUM and keep them updated with the latest version. A centralized antivirus system is functional at AUM to tackle viruses and Trojans. Additionally, a number of gateway firewalls and anti-spam technologies are also up and running in order to secure the internet and email communication of AUM users. Each device connected to the AUM network must have the necessary anti-virus protection. Devices which let malware etc. enter the internet will be prohibited from accessing the AUM network.

Software:

Each device and its software connected to the AUM network that is the property of AUM, will be supported by the appropriate IT staff. Administrator privileges are not given to users. Therefore, users should not be able to install non-sanctioned software on AUM devices. Software should not be downloaded or re-configured from the standard settings set up by the IT staff. Requests to install non-standard software should be made to the IT staff who may then relay the request to the IT Committee for approval.

Individuals who download or use software that is not part of the AUM software suite will be personally liable for the use of this software and all actions as a consequence of its use including but not limited to licensing agreements, illegal activities and damage. Deliberate or suspicious introduction of computer viruses or deletion or removal of software programs or files will be referred to the authorities for appropriate action.

Appropriate laws with respect to computer usage and copyrights are to be respected. No student, faculty, or staff member is permitted to copy or reproduce any licensed software or other copyrighted material on university computer equipment except as expressly permitted by license.

Hardware Support:

Support is provided for all core hardware and devices, including PC motherboards, peripherals, network interface cards, hard drives, storage devices, and the telephone system, provided that they are the property of AUM. All other devices, including peripherals, will not be supported and are the responsibility of the user. Hardware devices that are the property of AUM should only be examined and repaired by IT staff.

Classroom Technology:

The AUM IT staff provide support for faculty using technological devices in the classroom. This support is provided as necessary, either as routine maintenance or in response to specific

reports of malfunction. Classroom technology must never be moved from one location to another without the express written permission of the IT staff.

The IT staff will make themselves available to provide training to individuals or groups on the use of classroom technology or newly installed hardware or software. They will also retain necessary documentation and manuals for reference by authorized users of the classroom technology. In most instances, this is limited to instructors or senior administrators of AUM.

Rules to be followed in Computer Labs:

Food and drinks are not permitted inside the computer labs.

- Installation of any software that is not approved by the IT Committee is strictly prohibited.
- Reconfiguring the hardware configuration by unplugging the plugs and moving the hardware physically is prohibited.
- Downloading copyright protected video, audio, pictures, or other material from the Internet to a computer is prohibited.
- Messengers or any other chat services should be used for educational purpose only. No chatting is allowed during class hours.
- Installing or playing games, listening to streaming music, watching videos and similar activities on AUM devices are not allowed in the computer labs.

Storing Extremely Sensitive Data on Mobile Devices:

Only a handful of employees of AUM have been authorized to store extremely sensitive data on a mobile device, such as a laptop, CD or flash drive. Those authorized to store such data on a laptop computer have been issued or will be issued university laptops protected with biometric and encrypted security to use when storing such data. Storing such data on a mobile device, including laptops, without this authorization is a violation of university policy.

Electronic Mail:

One's personal e-mail, electronic files maintained on AUM equipment and personal web pages are part of a unique electronic information environment. This environment creates unique privacy issues that involve Maltese and international laws as well as AUM Policies:

- Most systems have public directories for temporary files. Examples are print spoolers, system wide web caches and scratch areas used by document editors. The temporary files stored in these directories are usually restricted to being readable only by the owner. To protect privacy and prevent these directories from overflowing, system administrators empty them regularly.
- IT staff reserve the right, to the fullest extent permitted by law, to inspect user files and communications for the purposes of investigating allegations of illegal activity, violations of AUM policies, or to protect the integrity and safety of network systems.
- E-mail shall not be considered as a secure vehicle. It is easily forwarded to a multitude of recipients and may be altered. Intruders to the network may be able to bypass your

password protection. The backup system may contain deleted e-mail for about 30 days. Mail undelivered for any reason may be copied to the mailbox of a ‘postmaster’ on the sender’s or recipient’s computers. For these reasons and others, one should not expect total privacy when considering your email messages.

- No user may intentionally read personal files, including those storing e-mail, without the owner’s consent. In the event of a lawful investigation of misconduct, law enforcement officials and University authorities involved in the investigation may inspect user files and communications.

World Wide Web:

The official AUM web pages contain public information about the University, its offerings, programs, and accepted obligations to students and the public. These pages project the public identity of the University and are its first electronic point of contact with the general public, students, parents, and employers. The University exercises strict editorial control over the content of its official web pages.

The University is not responsible for information, including photographic images, published on or accessible through personal web pages, including personal home pages. Personal web pages, created and maintained by employees, students or University- recognized student groups, are the sole responsibility of the person or student group identified by the account. The University does not monitor the contents of these personal web pages. The individual creating or maintaining personal web pages may be held liable for the materials posted on the web site. An individual who posts obscene material, for example, may be subject to criminal prosecution and an individual who posts copyrighted material might be liable to the owner of the copyrighted material under copyright law.

Personal web pages contain the personal expression of their creators. The contents, including link identifiers, of these pages include academic subjects, hobbies, religion, art, and politics as well as materials that some viewers may find offensive. Neither the contents nor the link identifiers are reviewed or endorsed by the University and shall not infer any ownership or endorsement by AUM.