AUM
AMERICAN UNIVERSITY OF MALTA

Policy: Computer Systems Usage

Policy Title	Computer Systems Usage
Policy ID	2024.17-v2-PTR_Po
Effective Date	June 2024
Responsible Office	Vice President for Administrative Affairs
Responsible Executive(s)	IT Office

Rationale:
The purpose of the Information Technology Usage Policy is for authorized users to have access to computers, programs, and files.

Scope:
All AUM employees

Policy:

Respect for the privacy of others is maintained unless access is explicitly authorized by those users. Theft, mutilation, or abuse of public or private computing resources violates the nature and spirit of the academic environment. Theft includes theft of services. Acts of theft will be referred to both the appropriate University authority and University Security.

Computer systems, software, applications and other resources are provided for the benefit of individuals within the AUM community. Deliberate or suspicious introduction of computer viruses or deletion or removal of software programs or files is a violation of computer usage policies. Acts of this nature will be referred to the appropriate University authority for action.

Central and network computer access are protected by password security. Protection of computer accounts is accomplished by not divulging one's password to others. If another user should gain access to one's password, the password should be changed immediately.

Usage

- Engaging in deliberately wasteful practices is prohibited. Printing large numbers of unnecessary documents is prohibited.
- Using the laser printer as a copy machine (printing multiple copies of a document), making unnecessary laser printouts (printing after every editing change is prohibited.
- Unnecessarily holding a public PC or workstation for a long period of time when other users are waiting for these devices is to be avoided.
- Computer connection in the faculty and staff offices is for use by authorized persons only.
- Activity on allocated computers is considered to be under the control of the assigned user.
- No server other than those implemented by AUM and the policies as ratified may be run

on AUM Network. This includes, but is not limited to, game servers, Windows Servers, Novell NetWare Servers, or any form of UNIX in a server configuration.

- University Policy prohibits users from sending threatening, obscene, or harassing messages to other users.
- The policy and practice of AUM is to respect the copyright protection given to software owners.
- 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
- Appropriate laws and copyrights are to be respected
- Requests for the duplication or installation of software will not be honored without proof of license or proof of purchase
- All faculty, staff, and student use of computers is governed by this guideline statement.

The policy and practice of AUM is to respect the copyright protection given to software owners. 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.

User Accounts and Personal Laptop Computers

Every student, faculty, and staff member at AUM is required to have a network user account consisting of an authorized user ID and a password in order to access University computing resources including access to the Internet. User accounts can be obtained from the Information Technology Department. New students are assigned an email address when they have completed the admissions process.

Personal laptop computers may be used on campus for educational purposes. Users must adhere to the rules and regulations of AUM as well as local and federal laws in the Republic of Malta. In order to obtain access to AUM computing resources, users must bring their laptop computers to the IT Department to register them.

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. Because it is impossible to anticipate all the ways in which individuals can damage, interrupt, or misuse AUM computing facilities, this policy focuses on a few simple rules. These rules describe actions that users should avoid and the principles guiding the rules. Each rule is followed by a list of actions that violate it.

1. Use AUM computing resources consistently within the stated priorities. The use of AUM computing resources follows these priorities:

   <u>High</u>: All educational, research and administrative purposes of AUM.
   <u>Low</u>: 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 e-mails; violating Maltese laws or AUM policies.

2. Accounts should be used only for legitimate purposes.

   Your account username identifies you to the entire international internet and intranet user community. You are held responsible for another person's use of your account. If someone using your username violates any policies, you may be held responsible. If you need to grant access to someone else to a file or other computer resource, work with IT to create an account for the person or assign access privileges to their account. If someone else offers you the use of an account that you are not authorized to use, decline. If you discover someone else's password, do not use it; report access of the password to the owner or to the IT Department. IT staff will never ask you for your password.

3. Honor 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 Department who carry out standard administrative practices, such as backing up files, cleaning up trash or temporary files, or searching for rogue programs, do not violate privacy.

   - Accessing the contents of files of another user without explicit authorization from that user is not permitted.
   - Intercepting or monitoring any network communications not explicitly meant for you is prohibited.
   - Use of the systems to transmit personal or private information about individuals unless you have explicit authorization from the individuals affected is not permitted. Distributing such information without permission from those individuals is also not permitted.
   - Creating or installing programs that secretly collect information about users is prohibited.
   - Software on AUM computing resources is subject to the same guidelines for protecting privacy as any other means for gathering information. Users are not allowed to use AUM computing resources to collect information about individual users without their consent. Note that most systems keep audit trails and usage logs (e.g., for ftp, login, object access etc); these are not secret and are considered normal parts of system administration.

4. Do not impersonate any other person.

Using AUM computing resources to impersonate someone else is wrong. If you use someone else's account without their permission, you may be committing acts of fraud because the account owner's name will be attached to the transactions you have performed. If, while using someone else's account, you communicate with others, you should clearly identify yourself as doing so. If you send anonymous mail or postings, you should realize that it is normal etiquette to indicate that your message is anonymous or is signed by a pseudonym. Because policy violators often use anonymous communication to hide their identities, many people give less credence to anonymous communication than to signed communication.

5. A University computer should not be used to violate any policies or laws.

Do not use AUM computing resources to commit violations of Maltese law or AUM policies. Examples are given below to assist you in avoiding inadvertent violations. This list is not comprehensive. In case of doubt, contact IT Department.

- Do not violate copyright laws and licenses. Many programs and their documentation are owned by individual users or third parties and are protected by copyright and other laws, licenses, and contractual agreements. You must abide by these restrictions; to do otherwise may be illegal.
- Do not extend the AUM network 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.
- Do not use AUM computing resources to attack computers, accounts, or other users by launching viruses, worms, Trojan horses, or making other attacks on computers on AUM or elsewhere.
- Do not perform unauthorized vulnerability scans on systems; such scanning is considered to be a hostile act.
- Do not use AUM computing resources to harass or threaten others.
- Do not use AUM computing resources to transmit fraudulent messages.
- Do not use AUM computing resources to transmit, store, display, download, print or intentionally receive obscene material, or to distribute pornographic material to minors. All users of AUM computing resources are subject to Maltese laws.

6. Taking computers or equipment off campus or out of the country. Only equipment or accessories issued to a faculty or staff member may be taken off campus. 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 return the equipment undamaged.

Compliance
First Warning

The Director of the IT Department sends a warning letter to alleged perpetrators of improper use of AUM computing resources. This warning ensures that the alleged perpetrators are aware that a policy violation has occurred and that there was a complaint. It offers a chance to avoid a repetition without having to admit guilt and a chance to secure an account against unauthorized use.

Second Warning

If a second offense occurs from an account that received a first-warning letter, after consultation with the VP for Administrative Affairs, the IT Department will issue a second warning and may require that the account holder be interviewed. The IT Department can authorize the temporary suspension of access to the user's account if the individual fails to attend the interview.

Disciplinary Procedures

If the previous two warnings do not convince perpetrators to desist, the matter is turned over to the IT Committee. The IT Department makes available all the information and evidence it has concerning the case to the IT Committee. After reviewing the case, the IT Committee recommends appropriate disciplinary actions to the Provost/President.

Computer Lab and Library Computer Lab Usage

All equipment in the computer labs is primarily used for academic purposes. When classes are not in session, students can use the labs for education purposes. Computer labs are open from 08:30 am till 5:00 pm from Monday through Friday and are available for classes as necessary. The library computer lab is open from 08:30 am till 7:00 pm, Monday through Friday, and reduced hours on Saturday and Sunday.

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 Department from CD, floppy disk, LAN, Internet, flash disks and the like is strictly prohibited.
- Reconfiguring the hardware configuration by unplugging the plugs and moving the hardware physically is prohibited.
- Having too many files on the computer affects performance of the PC. Students should notify the IT Department if performance of the computer is slow. The IT Department will check the complaint and will take the necessary action to resolve the problem.
- 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 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.

Extremely Sensitive Data‖ (aka ‘toxic data’) is defined as Data that, if accessed by unauthorized persons, could cause severe reputational, monetary, legal, or operational damage. Data in this category includes, but is not limited to classified or sensitive research, medical records, accusations or investigations of criminal activity, files of passwords to university systems, social security numbers, passport-type information, donation information and bank account and credit card PINs and passwords.

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 MALTA laws as well as AUM Policies:

- Users will be given a unique address for email. In case a user needs an alias to be created for his/her email address that is subject for approval from the Senior IT Manager.
- 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. One should never count on these files surviving after you log out from a computer.
- The IT Department reserves 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 is not secure. 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 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 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 criminally or civilly 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. If you feel you might be offended by material following a link identifier, or material on the page itself, you should not continue.