Computer and Network Use
Effective as of: 09.01.2021

American University of Armenia
Policy for Publication
Policy Number: ICTS20210005

---

1. Authorized Use

Use of the AUA computers, local network resources, electronic mail, Internet, web applications and remote computing, is to be consistent with the education, research, and service mission of AUA.

2. *Individual Privileges of Users*

AUA users have the following privileges conditioned upon acceptance of the accompanying responsibilities:

• Privacy

Electronic and other technological methods may not be used to infringe upon privacy. However, use of the computers and network is at each user's own risk because privacy cannot be guaranteed.

• Freedom from harassment and discrimination

• All members of the AUA community have the right not to be harassed or discriminated against through the computer or network usage of others. AUA policies and procedures on harassment, discrimination, publicity, hazing, non-academic student conduct and other related policies apply to use of the AUA owned or operated computing and network resources regardless of the medium used.

3. Individual Responsibilities of Users

Just as certain privileges are given to each member of the AUA community, each member is held accountable for his/her actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across the AUA establishes the trust and intellectual freedom that form the heart of the AUA academic community. This trust and freedom are grounded on each person developing the skills necessary to be an active and contributing member of the community. These skills include an awareness of and knowledge about information and the technology used to process, store, and transmit it. All users have the responsibility to report any discovered unauthorized access attempts or other improper usage of AUA computers, network, or other information processing equipment.

Common courtesy and respect for rights of others

Users are responsible to all other members of the AUA community in many ways that include but are not limited to:

• responsibly sharing AUA computing resources;

• respecting the rights of privacy for all, including, but not limited to, files of personal information and programs, no matter on what medium they are stored or transmitted. No user should look at, copy, alter, or destroy anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so;

• respecting the diversity of the population and opinion in the community;

• behaving ethically, and

• complying with all legal restrictions regarding the use of information that is the property of others. Users are responsible for recognizing (i.e., attributing) and honoring the intellectual property rights of others.

3.1. Responsible use of resources

Members of the AUA community are responsible for knowing what information resources (including, but not limited to, network) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources. Particular areas where users are expected to exercise responsible behavior include, but are not limited to, the following areas:

• Game playing: Playing games is prohibited at the AUA computer labs;

• Information integrity: It is the user's responsibility to be aware of the potential and possible effects of manipulating information, especially in electronic form, and to verify the integrity and completeness of information that is compiled or used;

• Use of desktop systems: Users are responsible in coordination with their Departments for the security and integrity of AUA information stored on personal desktop systems including, but not limited to, making regular disk backups, and controlling physical and network access to the machine. Users should not store passwords or other information that can be used to gain access to other AUA computing resources;

• Sharing of access: Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use of their accounts;

• Permitting unauthorized access: Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users;

• Use of privileged access: Special access to information or other special computing privileges are to be used in performance of official duties only. Information that a user obtains through special privileges is to be treated as private;

• Abusive Internet usage: Internet access can be used for job related matters only. Abusive downloading of third-party unlicensed programs, suspicious tools, games, photos, music and other entertainment files is prohibited;

4. Harmful activities prohibited at AUA

Harmful behavior that is subject to sanctions includes, but is not limited to, the following:

• Harassment: No member of the AUA community may, under any circumstances, violate AUA policies and procedures on harassment, discrimination, publicity, hazing, non-academic student conduct and other related policies through use of University -owned or operated computing and network resources. Nor shall any user intentionally disrupt or damage academic, research, administrative, or related pursuits; invade another person's privacy - academic or otherwise; or threaten such an invasion of privacy;

• Academic dishonesty: Users should always use computing resources in accordance with the ethical standards of the AUA community. Academic dishonesty (plagiarism, cheating) is a violation of those standards;

• Harmful activities: Harmful activities such as, but not limited to, the following, are prohibited: creating or propagating viruses; disrupting services; damaging files; and intentionally destroying or damaging equipment, software, or data belonging to AUA or other users. Further, users may not damage computer systems; obtain unauthorized extra resources; deprive other users of authorized resources; gain unauthorized access to systems by using knowledge of a special password, loopholes in computer security systems, or another user's password; or gain unauthorized access to resources used during a previous position at AUA;

• Denial of service: Deliberate attempts to degrade the performance of any computer system or network or to deprive authorized personnel of resources or access to any AUA computer system or network are prohibited.

• Accessing or attempting to access another individual's data or information without proper authorization (e.g., using another person's password to look at their personal information);

• Obtaining, possessing, using, or attempting to use someone else's password without proper authorization;

• Tapping phone or network lines (network sniffers);

• Making more copies of licensed software than allowed;

• Sending an overwhelming number of files across the network (e.g., spamming or e- mail bombing);

• Intentionally releasing a virus or other program that damages, harms, or disrupts a system or network;

• Intentionally preventing others from accessing services;

• Unauthorized use of the AUA resources;

• Sending forged messages using someone else's identity;

• Using AUA resources for unauthorized or illegal purposes;

• Unauthorized access to data or files even if they are not securely protected.

5. Constrained activities at AUA

Policies listed below have specific application to constrain the types of activities that may be carried on by users of AUA computers and network. AUA constrained behavior includes, but is not limited to, the following:

• Use of copyrighted information and materials: Users are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other material;

• Use of licensed software: No software may be installed, copied, or used on AUA resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, terms of license, etc.) must respect the contractual agreements;

• Political campaigning: The AUA does not permit use of AUA -owned or operated computers and network resources for activities that might be construed as political campaigning;

• Commercial advertising: The AUA does not permit use of AUA -owned or operated computer and network resources for commercial advertising;

• Personal business: Computing facilities, services, and network may not be used in connection with compensated outside work or for the benefit of organizations or individuals not related to AUA, except in the cases of incidental use, use supporting scholarly pursuits, or other use subject to arrangements between the user and the user's dean, director, or supervisor. Incidental use for personal business includes occasional communication and other use that has negligible effect on the use of technology by others;

• Network installations: Users may not, without authorization from the ICTS Department, connect any network equipment to the AUA network. Network equipment includes, but is not limited to , routers, firewalls, switches, WiFi access points or any devices that provide network connectivity to more than one individual computer system. In addition, users may not connect to the network any computer that is configured to perform the functions of the aforementioned network equipment;

• Anonymous usage: Users may not run network services that allow the anonymous deposit of data on the AUA network. For any such data transfer services, security must be provided through usernames and passwords that are traceable to individual users.

6. Control Mechanisms over Computer and Network Use

6.1. Control of access to information

AUA may control access to its information and the devices on which it is stored, manipulated, and transmitted.

6.2. Imposition of sanctions

AUA may impose sanctions on those who violate AUA policies applicable to computer and network usage.

6.3. System administration access

The AUA System Administrator may access others' files or accounts for the maintenance of network and computer and storage systems, such as to create backup copies. The AUA System Administrator may access others' files or accounts to investigate allegations of misconduct, violation of AUA policy or procedure. In all cases, however, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

6.4. Suspension of individual privileges

The ICTS Department may suspend computer and network privileges of an individual for reasons relating to the safety and well-being of members of the AUA community or AUA property or for reasons relating to the violation of AUA policies. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the VP Operations/COO , or the Human Resources Office.

7. Enforcement of the Appropriate Use Policy

7.1. Investigative contact

If an AUA employee is contacted by a representative from an external organization who is conducting an investigation of an alleged violation involving AUA computing and networking resources, the user must inform the office of the Vice-President immediately. The employee must refer the requesting agency to the Vice-President who will provide guidance regarding the appropriate actions to be taken.

7.2. Responding to security and abuse incidents

All AUA users and departments have the responsibility to report any discovered unauthorized access attempts or other improper usage, as described in “Harmful activities prohibited at AUA” and “Constrained activities at AUA” sections above, of AUA computers, network, or other information processing equipment. If a user observes or receives a report of (other than as in “Investigative Contact” section above), a security or abuse problem with any AUA computer or network facilities, including violations of this policy, the user must:

• Take immediate steps to ensure the safety and well-being of information resources. For example, the AUA System Administrator should be contacted to temporarily disable any apparently compromised computer accounts or to temporarily disconnect or block offending computers from the network;

• Ensure that the AUA System Administrator and the user's department head are notified.

Once notified, ICTS will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded to the Director of ICTS.

7.3. Range of disciplinary sanctions

Persons violating this policy are subject to sanctions, such as loss of computer or network access privileges, disciplinary action, up to and including, but

not limited to, dismissal from AUA or legal action. Some violations may constitute criminal offenses, under local laws. AUA will carry out its responsibility to report such violations to the appropriate authorities.

7.4. Appeals

Appeals should be directed through existing procedures established for employees and students.