THE AMERICAN UNIVERSITY 55 of PARIS YEARS

COMPUTING & NETWORKING RESOURCES ACCEPTABLE USE

Policy Number: IT001EN
Last Review: 29 Jan 2019

1. PURPOSE
AUP owns its computing and telecommunications networks, computing equipment, and computing & networking resources (see Definitions) and provides them to support the academic and administrative functions of the University. This policy ensures that the use of computing, network, and information technology resources is safe, secure, and compliant with applicable laws.

2. WHO IS AFFECTED BY THIS POLICY
All users of AUP computing resources (employees, applicants, students, alumni, visitors, contractors, consultants, and other workers at AUP affiliated with third parties).

3. POLICY STATEMENT
AUP policies and procedures govern the use of AUP infrastructure and information technology equipment. Departments or units may adopt additional rules to meet specific administrative or academic needs. Any adopted requirements must be in compliance with this policy and applicable laws.

3.1 **Access to Information Technology Resources**

Access to AUP Resources requires the approval of an appropriate AUP official or department. Any member of the AUP Community may use AUP's information technology resources in support of instructional, research, and service missions sanctioned by AUP. Access to these resources is granted to each individual for a specific purpose. Proper use of the resources must be consistent with that purpose. In particular, instructional access is granted for work done by officially registered students in support of a recognized course of study. Research access is granted for work approved by an authorized official of a University department.

Please note that additional information on the creation and management of network accounts and the use of passwords is available in specifically dedicated policies - Network Account (IT003EN) and Password Management (IT005EN).

1. **Faculty and Staff** access to AUP Resources is authorized by The Office of Human Resources (HR). Only instructions from HR to the ITS Department will result in the creation, modification, or deletion of any credential related to a faculty or staff member, such as User IDs and passwords.

2. **Student** access to AUP Resources is authorized by The Office of the Registrar. A student account is automatically created when the student status is changed to “Admitted”. The automated process will create the necessary student credentials, including User IDs and password.

3. **Visitor** access to AUP Resources is generally limited to the wireless network and Computer Kiosks. Requests for visitor access to these resources must be submitted and justified by an AUP staff member. This includes access for special events or other unique circumstances. AUP will grant visitor access to AUP Resources for a limited time as defined by the requestor.

4. **Commercial Activity:** University information technology resources may not be used for any commercial activity. Prohibited commercial activity includes using either e-mail or the web to advertise a service or activity that is not considered non-profit under the French tax code. Publishing your CV is normally not considered a commercial activity. Publishing a "link" to an external commercial site is normally not considered a commercial activity, unless you are compensated for publishing it. AUP reserves the right to decide whether or not any given activity is commercial, and AUP's decision is final.

5. **Respecting US & French law**: By using University-supplied information technology resources and associated facilities, individuals and other entities agree to abide by all policies and procedures adopted by AUP, as well as all current and pertinent US and French laws. These include, but are not limited to, University policies and procedures against harassment, plagiarism, and unethical conduct, as well as laws prohibiting theft, intellectual property and copyright infringement.

6. **Restricting or Limiting Access**: AUP reserves the right to restrict the use of its information resources and facilities, and to limit access to its computer systems, subscribed Cloud Services, and networks, when faced with evidence of violations of University policies or standards, of contractual obligations or of other applicable laws. AUP also reserves the right to remove or limit access to material posted on or transmitted by its computers and network facilities.

   ITS has the authority to disconnect from the network any device which may impair or disable the network, compromise the integrity of other network-connected devices, threaten the security of university data stored on the network, or be used for activities which violate AUP policies.

3.2 Acceptable Use Guidelines for Computer, Cloud Services and Network Facilities

AUP strives to provide fair and distributed access to information technology resources (i.e., computers and wired/wireless networks) and facilities for a large number of users. The acceptable use guidelines which follow apply equally to all types of electronic information services, including electronic mail (e-mail) and electronic news groups provided on AUP's computer and network facilities. Everyone using University information technology resources is responsible for following guidelines.

Acceptable use:

1. complies with all applicable laws and respects University regulations and policies.
2. follows the same standards of common sense, courtesy, and restraint that govern the use of other public facilities.
3. requires users to be ethical and respectful of the rights of others and of the diversity of the AUP Community.
4. respects individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance.
5. respects identification and security mechanisms that prevent unauthorized access. Access authorization relies on user identification and a password for each user. The ITS ID (NetID) forms the basis for mechanisms that are designed to establish ownership and responsibility for computing resources and use.
6. requires that all users refrain from any illegal and improper intrusions into the accounts of others and/or into any University information technology resources and systems.
7. recognizes and honors the intellectual property rights of others.
8. respects all software licenses and/or purchase agreements; if you have not met the conditions of such an agreement for a given software package, do not copy the package for your use.
9. of all off-campus network connections, i.e., use of the Internet, respects AUP's network access contracts that impose strict requirements. In general, off-campus network use must be for education or research. AUP's access contracts prohibit commercial activities such as advertising.
10. does not state or imply AUP sponsorship or endorsement.
11. does not overload AUP computing equipment or systems, or otherwise harm or negatively impact the system's performance, or congest the network.
12. requires that all material prepared and utilized for work purposes and posted to or sent using University computing and other telecommunicating equipment, systems or networks must be accurate and must correctly identify the creator and receiver.

Regulatory Limitations

1. AUP may monitor access to its equipment and networking structures and systems for the following purposes:
   a. To ensure the security and operating performance of its systems and networks.
   b. To enforce AUP policies.
2. AUP reserves the right to limit access when AUP policies are violated or when AUP contractual obligations or operations may be impeded.
3. AUP may authorize confidential passwords or other secure entry identification. However, the users of the AUP computing resources should have no expectation of privacy in the material sent or received by them using AUP computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above.
4. Except for reasons stated above, AUP generally does not monitor or restrict material residing on AUP computers housed within a private domicile or on non-AUP computers, whether or not such computers are attached or able to connect to campus networks.
5. All material prepared and utilized for work purposes and posted to or sent using AUP computing and other telecommunicating equipment, systems or networks must be accurate and must correctly identify the creator and receiver of such.

3.3 **E-Mail: Notes on use, Content and Confidentiality**

AUP encourages appropriate use of e-mail (electronic mail) to enhance productivity through the efficient exchange of information in furtherance of AUP's mission. Use of e-mail should be consistent with this policy and guidelines based on common sense, common decency, and civility applied to the network computing environment.

Unless otherwise prohibited by law, AUP may send official communications to employees and enrolled students via the portal or by email with the full expectation that such communications will be read by the recipient in a timely fashion.

AUP provides every student and employee with an email account and a portal to access AUP communications. For more information see: My Account

AUP is not responsible for the delivery failure of email, including attachments, forwarded to any non-AUP email address. Communications may be time-critical, and employees and students are expected to review messages received through AUP email on a frequent and consistent basis. Individuals are subject to policies and directives communicated via email, even if they do not read the messages. Individuals must ensure that there is sufficient space in their accounts to allow for email to be delivered.

Official email communications from AUP will be sent to the AUP email address of students, faculty and staff. Email communication sent to AUP must be sent from official AUP email addresses.

Individuals who choose to forward e-mail from an AUP e-mail account to a different e-mail address (e.g. Hotmail, Gmail, Yahoo, etc.) do so at their own risk. AUP is not responsible for e-mail, including attachments, forwarded to any non-AUP e-mail address. Automatic email forwarding introduces the potential for unauthorized disclosures of sensitive information.

AUP's Information Technology Services staff makes every reasonable attempt possible to maintain the confidentiality of e-mail correspondence. However, the improper use of such a system could result in a disruption of service and AUP reserves the right to take any necessary steps for the resolution of such a matter, including opening any electronic message.

3.4 **Wireless Access**

The American University of Paris is solely responsible for authorizing, managing and auditing connections to the AUP Network, including the security and integrity of the network and related systems. Records and logs are recorded per the *"Décret du 26 Mars 2006 N°2006-358 relatif à la conservation des données des communications électroniques"* and contains the following information: user identification, connection date and times, MAC and IP address of the terminal, service or website accessed. These logs are stored for one year, and may be communicated to the French legal authorities at their request.

AUP provides wireless network access to invited users, including clients and visitors. This access is provided on an "as is" and "as available" basis. AUP does not guarantee that this service will be uninterrupted, error free, or free of viruses or other harmful components. AUP cannot control material, information, products or services on the internet. Users should be aware that there are security, privacy, and confidentiality risks inherent in wireless communications and technology. AUP does not make any assurances or commitments relating to such risks. By using AUP's wireless network, users waive any potential claims against AUP arising from use of this service.

Network access is provided only as a courtesy and may or may not be available at any requested time. AUP reserves the right to deny or restrict access to any user for any reason, including but not limited to abuse of the network, excessive bandwidth consumption, or using the network for any type of criminal activity. All wireless infrastructure devices that reside at AUP sites and/or connect to the AUP network (e.g. Eduroam), or provide access to information classified as Confidential, Highly Confidential, or Restricted must:

1. Be installed, supported, and maintained by an approved support team.
2. Use the AUP approved authentication protocols and infrastructure.
3. Use the AUP approved encryption protocols.
4. Maintain a hardware address (MAC address) that can be registered and tracked.
5. Not interfere with wireless access deployments maintained by other support organizations.

Such requirements also apply to all lab wireless infrastructure devices that provide access to Confidential, Highly Confidential, or Restricted information. Lab and isolated wireless devices that do not provide general network connectivity to the AUP network must be isolated from the AUP network (i.e. must not provide any connectivity to the AUP network) and comply with AUP network policies.

3.5 **Information Security: An Additional Note of Caution**

All users of the various computing systems maintained and operated by AUP should be aware of the limited security of these systems and of information stored there. AUP's systems serve a variety of academic users and are intentionally open systems to make access and operation easy for users. Security for each computer system is essentially user-controlled by means of access passwords and guarding features.

These security methods provide for orderly operation of each computer, but place the responsibility for security upon the user. Users should realize that unauthorized access to information is possible through malicious mischief and by carelessness about protection of passwords and the use of system security features. Users should be careful about storing or processing sensitive information; AUP cannot guarantee protection from unauthorized access.

3.6 **Access to Administrative Systems and Data**

The users of the AUP computing resources are informed that to the extent necessary for the accomplishment of their missions, or the accomplishment of its missions by AUP, the personal data of the users of the AUP computing resources and the AUP systems might be accessed by the French or American administrative authorities. Such access or disclosure shall be made in accordance with the applicable laws and policies.

3.7 **Application of Public Records Law**

All information created or received for work purposes and contained in AUP computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records Law applies (US, French or European PRL).

3.8 **Computer Software Supported**

Any member of the AUP Community who has been granted the use of AUP information technology resources, can expect support for the usage of any supported software and operating systems. See the ITS Department for a complete list of supported software and operating systems. No support will be provided for home or personal computers or software.

3.9 **Enforcement and Violation of Policy**

Any violation of this policy is "misconduct" as defined by the AUP Code of Student Conduct or as defined by Office of Human Resources policies. If the Director of Information Technology Services believes that a user has violated this policy, s/he may refer the matter to the relevant campus disciplinary channels. AUP will investigate and may take action to prevent further occurrences. During an investigation, AUP reserves the right to copy and examine any files or information resident on University, or cloud-based, systems, allegedly related to improper use, including the contents of electronic mailboxes.

Investigations that uncover improper use may result in sanctions that could include one or more of the following:

1. Revocation or suspension of access privileges;
2. A written warning or reprimand;
3. Disclosure of information found during the investigation to other AUP authorities;
4. Installation of automatic measures to limit improper use;
5. Demotion, suspension without pay, or dismissal;
6. Violations of law may be referred for criminal or civil prosecution;
7. Disciplinary actions and termination of employment.

4. RESPONSIBILITIES

The Director of Information Technology Services is responsible for the interpretation and administration of this policy.

5. DEFINITIONS

AUP, the University	The American University of Paris
AUP Code of Student Conduct	The statement of rules and regulations governing student conduct as established by the University official.

ITS	Department of Information Technology Services at AUP
AUP Community	Faculty, staff, students, and alumni of AUP, whether or not compensated for their services; persons performing research or engaging in work or study utilizing AUP Resources or facilities; and other persons allowed access to AUP Resources or facilities.
AUP Resources	Facilities, library resources, equipment, funds, personnel, and other resources belonging to or supplied by AUP.
User	A person expressly authorized to use University information technology resources and associated services provided by AUP.
User ID or NetID	A unique identifier for each user that permits authorization and access to AUP computer resources when used with the correct password.
Computing & networking resources	Facilities, computing equipment and technologies required to accomplish information processing, storage, and communication, whether individually controlled, shared, stand alone or networked. Examples include classroom technologies and computing and electronic communication devices and services.
Cloud Services	Any service (i.e Office 365) made available to users on demand via the Internet from a cloud computing provider's servers.
Computer Kiosks	Computers for quick and self-service access.
Confidential Information	University information, technical data, know-how and other information which is not otherwise in the public domain and of which the owner actively undertakes to restrict or control the disclosure to Third Parties in a reasonable manner.
Highly Confidential Information	Information containing research, educational, enterprise or personally identifiable data that if released could result in critical or serious financial, reputation or legal impact to the University or an affiliated organization or individual. Example include medical records.
Restricted Information	Information containing research, educational, enterprise and/or personally identifiable data that if released could result in modest financial, reputation or legal impact to the University or an affiliated organization or individual. Examples include student records or analytics data, staff records, unpublished research reports or data, and audit reports.
MAC address	The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

6. APPROVALS & HISTORY
    - Approved by the Leadership Team on June 1, 2012.
    - Enhancements to language, formatting on August 24, 2012.
    - With feedback from Tracy Mitrano, Director of the IT Policy and Institute for Computer Policy and Law at Cornell University on October 8, 2012.
    - Edited and merged with older policies March 15, 2018.
    - Approved by the Leadership Team on January 29, 2019.
    - Next review November 2022.

7. ISSUING OFFICE AND CONTACT

Ali Rahimi
Director of Information Technology Services
2 bis, Passage Landrieu
75007 Paris
+33 1 40 62 06 96
helpdesk@aup.edu