INFORMATION TECHNOLOGY RESOURCES RIGHTS, PRIVILEGES, & ACCEPTABLE USE

Policy Number: IT001EN
Last Review: 1 February 2023

1. PURPOSE

AUP owns its information technology resources, including computing and telecommunications networks, computing equipment, and information resources (see Definitions). The university provides these resources to support the academic and administrative functions of the institution, and it expects the responsible use of the same. All users of the university's information technology resources are expected to demonstrate the highest respect for the rights of others in their use of these resources. This policy defines these expectations to ensure 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). This policy applies to all information technology resources provided by the university and to all users of these resources. All members of the university community are given notice of this policy by virtue of its publication and are subject to it on the same basis. All users are expected to familiarize themselves with the contents of this policy and act in conformance with the following principles regarding any use of the university's IT resources.

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 comply with this policy and applicable laws.

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.

3.1 Rights

AUP protects the rights guaranteed to users of the IT resources through relevant French and American regulatory and legal bodies. These rights pertain to data, for example, that is protected by the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA), and General Data Protection Regulation (GDPR) as well as Copyright, Harassment, and other, similar legal protections.

3.2 Privileges

AUP provides:

1. Access – fair and distributed access to information technology resources, services, and facilities according to their role and level of authorization.

2. Protection – identification and security mechanisms designed to establish ownership and responsibility for computing resources, data and information, and services and prevent unauthorized and unethical access and conduct.
3. Standards – guiding principles for behavior and conduct (See Acceptable Use section below), service selections, levels of performance (See ITS website for Service Level Agreements or SLAs), equipment (See ITS website for current standards for hardware and software), and processes (See ITS website for access to request forms and workflow).

3.3 Acceptable Use Guidelines for IT Resources

AUP strives to provide fair and distributed access to information technology resources, services, and facilities for all users with approved access. The acceptable use guidelines which follow apply equally to all types of electronic information services 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 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.
9. Respects AUP's network access contracts that impose strict requirements of off-campus network connections. In general, off-campus network use must be for education research and administrative tasks. 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.

3.4 Expectations for Conduct and Behavior

Users of the university's IT resources should observe the same standards of ethical conduct and courteous behavior that govern non-electronic vocal and written communications and other personal interactions. Ethical and courteous use of information technology resources is the responsibility of every user. This principle is fundamental to the spirit of community and standards of civility that should govern interactions among all members of the university community.

The university's commitment to the principle of fair and equitable access for all users seeks to ensure that no member's use of resources compromises the access of other members to shared resources, including equipment, services, and budgets. The principle requires that users refrain from activities that compromise its overall ability to deliver IT services or that interfere with its ability to make IT resources available for all qualified users. The

university reserves the right to take all appropriate and reasonable measures, including the use of available technological interventions to ensure equitable access to IT resources for the benefit of all users.

Employees of the university also have a special ethical duty to use their broad access to the university's information technology resources in conformance with this and all other principles of this policy. Use of information technology resources by university employees that is unrelated to their official position should be reasonable and limited in both time and resources and must not interfere with university functions or the employee's performance of employment responsibilities.

Any attempt to compromise data or information systems will be considered as a violation of expectations for Conduct and Behavior.

Investigations of suspected violations may be referred to third-party contractors acting as agents of the university. Violations of this principle may result in limiting or even denial of access to these resources, as well as student and/or employment disciplinary action.

3.5 Expectations for Privacy

The privacy of all users and the integrity and operational security of the university's information technology system must be respected by all members of the university community. University IT resources must not be used to attempt unauthorized access to information maintained by users or by the university itself. This principle is intended to apply to all aspects of the university's information technology system, and to all users, whether students, employees, or guest users.

Electronic records sent, received, or stored on computers owned, leased, or administered by the university are the property of the university. As the property of the university, the content of such records is subject to inspection by university personnel. While the university does not routinely do so, the university is able and reserves the right to monitor and/or log all network activity of users without notice, including all email and Internet communications, in the process of protecting university information. Investigations of misuse, unauthorized use, or illegal activity, as well as routine or emergency maintenance of the university's IT system, may require observation of communications or information by appropriate and authorized university officials, employees, or their authorized agents. Such activities are not in violation of this principle so long as these activities are conducted by authorized individuals on behalf of the university. University employees conducting these activities are required to sign a confidentiality agreement. Other authorized agents of the university are subject to contractual language requiring the protection of university data.

If an employee marks a set of data as personal, AUP will not have the authorization to access it.

Any request to access data, including email and Microsoft 365 content, associated with another employee’s account must be approved by HR. If the account is associated with a student, the request must be approved by the Dean of Student Development.

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 such computers are attached or able to connect to campus networks.

Unauthorized access to information constitutes a violation of this policy and may result in serious disciplinary sanctions under policy AA014, up to and including expulsion, and/or employment discipline, up to and including termination. Violation of this principle may also constitute a violation of French law.

3.6 Acceptable Use of Access Privileges

Access to AUP Resources requires the approval of an appropriate AUP official or department and is granted for a specific purpose relevant to the instructional, research, and service missions sanctioned by AUP. Proper use of the resources must be consistent with that purpose. 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 one's CV is normally not considered a commercial activity. Publishing a "link" to an external commercial site is normally not considered a commercial activity unless one is compensated for publishing it. AUP reserves the right to decide whether any given activity is commercial, and AUP's decision is final.

User access to information technology resources is granted to an individual by the university solely for the grantee's own use. User access privileges must not be transferred or shared, except as expressly authorized by an appropriate university official (see below). This principle is intended to help protect the integrity, security, and privacy of user accounts. Sharing access with another individual undermines the security of an account, leaving it vulnerable to abuse by others, and may further jeopardize the security of the university's information technology system.

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 , 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 "Confirmed". 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.

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.

For information and assistance about obtaining and/or maintaining a university IT account, contact the university's IT Service Desk at itservices@aup.edu. 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 (IT004EN).

3.7 Acceptable Use of E-Mail Privileges

AUP provides every student and employee with an email account and a portal to access AUP communications. 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.

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. 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. AUP is not responsible for the delivery failure of email, including attachments, forwarded to any non-AUP email address.

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 does not prohibit but does not encourage this practice. 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, and emails or files marked "private" are afforded extra confidentiality. 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 copying, archiving, and inspecting any electronic message or file suspected to be harmful.

3.8 Acceptable Use of Network Privileges

AUP provides network access to authorized users. 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 network communications and technology. AUP does not make any assurances or commitments relating to such risks. By using AUP's 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 network 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 infrastructure devices that provide access to Confidential, Highly Confidential, or Restricted information. Lab and isolated devices that do not provide general network connectivity to the AUP network must be isolated from the AUP network (i.e., it must not provide any connectivity to the AUP network) and comply with AUP network policies.

AUP 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: 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.

3.9 In the Case of Misuse

Users must not use university information technology resources in the commission of any unlawful or otherwise unauthorized act. Violation of French law, including anti-hacking provisions, copyright, and trademark laws, is inconsistent with ethical and responsible use of university IT resources and is strictly prohibited. In addition to

possible civil and criminal penalties, illegal use can result in serious sanctions under the university policies AA033 (ARC GDPR and Copyright), SS07 (Student Rights) and SS08 (Student responsibilities). Sanctions can include severe employment discipline, up to and including termination GO005 (Internal Regulations). The university will cooperate fully with law enforcement officials regarding criminal investigations of any use of its IT resources in violation of this principle.

Investigation

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.

When the Chief Information Officer, a designee, or the appropriate system administrator has reason to believe that a violation involving a security threat to the system or other users and/or illegal activity may have occurred, he or she may immediately suspend information technology privileges for the involved user(s).

Investigations of suspected violations may be referred to third-party contractors acting as agents of the university.

If a user account is summarily suspended, the university will attempt to notify the user immediately. Users may check the status of reinstatement of access privileges by contacting the university's IT Help Desk at +33 1 40 62 06 96 or itservices@aup.edu. If, upon further investigation by the appropriate university officials, the violation appears to have been willful and deliberate, the appropriate university official may refer the violation and the violator's identity to the appropriate university authority for disciplinary action.

Violation

Violation of this policy will result in action by the appropriate university office or agency. Students who violate this policy may be referred to the university's Office of Student Conduct for disciplinary action under the [Code of Rights]. Employees who violate this policy may be subject to disciplinary measures imposed by their appropriate supervisor in consultation with the university's Human Resources Office. Violations of French law regarding unlawful access or use may be referred to the appropriate law enforcement officials for investigation and/or prosecution.

Sanction

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, archive, and inspect 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. Suspension or expulsion for students and
6. Demotion, suspension without pay, or and termination for employees;
7. Violations of law may be referred for criminal or civil prosecution; and,
8. Disciplinary actions and termination of employment.

University sanctions will be imposed by the appropriate university authority upon findings made in conformance with the procedures outlined in applicable university policies.

Sanctions may also include restitution to the university for charges incurred in detecting and substantiating violations of these rules, as well as any costs incurred because of the violation itself. Users should be aware such charges could be substantial.

3.10 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 depends on user controls 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 activity 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.

3.11 Computer Software Supported

Any member of the AUP Community who has been granted the use of AUP information technology resources, whether on premises or in the "cloud," can expect support only for the usage of software and operating systems on the ITS Department site list of supported software, services, and operating systems. No support will be provided for home or personal computers or nonstandard software, whether installed on a university-managed computer or on a home or personal computer.

4. Frequently Asked Questions

What are activities that may violate the statement of Acceptable Use of Access Privileges?

Examples of activities that may violate this principle include, but are not limited to, the following:

1. Hacking or attempted hacking activity of any kind, including but not limited to:
    a. Altering, damaging, or attempting to alter or damage files or systems without authorization
    b. Intentionally damaging or destroying the integrity of electronic information
    c. Attempting to access or control another computer network without authorization
    d. Scanning of networks for security vulnerabilities
2. Unauthorized access of another user's account in any manner
3. Unauthorized viewing of information maintained on university systems
4. Unauthorized publishing, sharing, or disseminating information from university systems without appropriate authorization

What are activities that may the Statement of Ethical Conduct and Behavior?

Examples of activities that may violate this principle include, but are not limited to, the following:

1. Intentional Disruption of the IT System, such as installing, propagating, or otherwise running any malicious program that attempts to violate the operational integrity of the system; unauthorized interception of electronically transmitted information; acquiring or attempting to acquire the passwords of other users; unauthorized deletion of another user's postings, files, or information; intentional physical damage to university-owned IT resources; hacking activity of any kind; unauthorized connections to the system, its networks, as well as unauthorized extensions or re-transmissions of any system services; and, failure to comply with requests from appropriate university employees to discontinue activities that threaten the operational integrity of any component of the IT system.
2. Inequitable Use of IT Resources, such as downloading or uploading large files during periods of peak usage after having received a request from the appropriate university IT official to defer such use until a later time.
3. Misrepresentation, such as misrepresentation of one's identity or of the identity of the sender of an electronic communication or web site host, obscuring or forging of the date, time, physical source, technological source, or other header information of a message or transaction, alteration of the content of a message originating from another person or computer with the intent to deceive.

4. Harassment, such as the electronic distribution of threatening or illegally harassing communications, repeated, unsolicited, or unwanted electronic communication with an individual after the sender has been asked to stop.
5. Unauthorized Use, such as using IT resources while on duty for the university in a manner that interferes with performance of employment responsibilities, inappropriate use of university authority or special access privileges to the university's system.
6. Commercial Use, such as using university hosted IT services to advertise, provide services to, and/or sell commercial products or services or using university IT resources to distribute unsolicited advertisements on behalf of commercial entities.
7. Copyright Violation, such downloading any copyrighted media without permission from the copyright owner, creating a copy of electronic media that has been purchased and making it available online to others, installing software that stores, downloads, uploads, advertises content, and distributes copyrighted media without permission from the copyright owner, unauthorized storage of copyrighted materials, including documents, software, music and films, on university owned or controlled IT resources, and posting to personal web space licensed software that has been modified to run without a license.

5. RESPONSIBILITIES

The Chief Information Officer is responsible for the interpretation and administration of this policy.

6. 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.

AUP Community
Faculty, staff, students, and alumni of AUP, whether compensated for their services or not; 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.

Cloud Services
Any service (e.g., Office 365) made available to users on demand via the Internet from a cloud computing provider's server.

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.

Hack
Unauthorized access to a computer or service. This access may include modifications to programs or other unauthorized activities.

Information, Confidential
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.

Information, Highly Confidential
Information containing research, educational, enterprise or personally identifiable data that if Information released could result in critical or serious financial, reputation or legal impact to the University or an affiliated organization or individual. Examples include medical records.

Information, Restricted
Information containing research, educational, enterprise and/or personally identifiable data that if released could result in financial, reputational, 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.

ITS
Department of Information Technology Services at AUP

Kiosk
Public computer for quick and self-service access.

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.

Malware
Software designed to negatively impact or impair the performance of computers or networks. May include intrusive pop-up ads, malicious and/or damaging software, virus programs, worms, Trojans, scareware, and ransomware. May result in loss or theft of data. Eradication may require use of specialized tools or complete erasure and rebuilding of computer operating system. May be introduced by opening dubious email attachments, visiting malicious websites, or installing infected software.

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.

6. RELEVANT LINKS

Family Educational Rights and Privacy Act (FERPA): www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Health Insurance Portability and Accountability Act (HIPAA): www.hhs.gov/ocr/hipaa/
Gramm-Leach Bliley Act (GLBA): www.ftc.gov/privacy/privacyinitiatives/glbact.html
National Commission for Computing and Liberties (CNIL): https://www.cnil.fr
General Data Protection Regulation (GDPR): https://gdpr.eu/

7. 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 February 7, 2023.

- Next review February 2024.

8. ISSUING OFFICE AND CONTACT

Chief Information Officer
Information Technology Services
69 quai d’Orsay
75007 Paris
+33 1 40 62 06 96
itservices@aup.edu