The American University of Paris

DATA RESOURCES, ACCESS, CLASSIFICATION, AND USAGE

Policy Number: IT005EN
Last Review: 9 Nov 2023

1. PURPOSE

Information is one of the university's most valuable assets, and its value is increased through widespread and appropriate use. The university grants access to the greatest extent possible while recognizing the responsibility to secure data appropriately. Consistent with the university's obligation to preserve and protect such information by all appropriate means, access to information is made available only where there exists a valid business purpose.

The university, as the owner of all data, delegates responsibility for its oversight to the Chief Information Officer (CIO). 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 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 data and information resources is safe, secure, and compliant with applicable laws.

2. WHO IS AFFECTED BY THIS POLICY

All users of AUP data and information resources (employees, applicants, students, alumni, visitors, contractors, consultants, and other workers at AUP affiliated with third parties). This policy applies to all information 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 data and information resources.

3. POLICY STATEMENT

AUP policies, processes and procedures govern the use of AUP data and information. 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 data and information resources, individuals and other entities agree to abide by all policies, processes 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.

User access to data and information 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.

This principle is intended to help protect the integrity, security, and privacy of data and information. 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 data and information system.

The scope of data access includes the following:

- All data and systems supporting the business and operational needs of the university.

- Information and data in all forms, including but not limited to, information processing activities, computerized data (whether stored on university-managed servers and storage, storage area network, local servers, personal workstations or storage devices, or vendor-provided infrastructures such as a "cloud"), and manually maintained data files regardless of where those files are stored.
- All application, network, and operating system software used for computerized management of these data or systems.
- Computerized data-processing activities related to research and instruction where the CIO determines that such activities should be covered by this policy.
- All data and systems owned by or within the control of the university.

3.1 Access

The university determines levels of access to data and systems according to principles drawn from various sources such as French law, university regulations, and ethical considerations. Individuals accessing university data and systems must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in use. Users will be required to complete security awareness and compliance training before access will be granted. All university data must be protected in accordance with policy. See IT002EN Information Security.

In accordance with policy regarding separation from the university, supervisors are responsible for notifying Human Resources prior to employee separations to ensure timely removal of access to administrative systems, university-provided email, and other university resources. Human Resources is responsible for updating appropriate personnel data and notifying Security Officers and other relevant departments of employee separations on or before the last date of employment, or as soon as possible upon notification of employee separation.

Data Security Officers are responsible for maintaining procedures related to granting, modifying, and revoking access to administrative system data. Upon approval by the appropriate university official, Data Security Officers are responsible for maintaining (including granting, modifying, and revoking) access to administrative systems (e.g., modules within the student information system and other systems, such as HR, Finance, and Student). Data Security Officers are required to sign appropriate confidentiality agreements. Data Security Officers report to the following university officials:

Data	**University Official**
Student Records Data	Registrar
Student Health, Accommodations, Activities, Conduct, and Services Records	VP for Student Services
Financial Aid Data	Director of Financial Aid
Admissions Data	Vice President for Admissions
Finance Data	EVP for Finance and Operations
Human Resources Data	Director of Human Resources
Alumni and Development Data	Director of Advancement

Access to university data and systems is granted to individuals with whom the university has an active affiliation (e.g., students, faculty, staff, guests, vendors, etc.). Under unusual circumstances, access may be granted or revoked by request of the CIO in consultation with university management. Examples of when access may be revoked include, but are not limited to:

- Situations that require immediate action to protect university data, systems, or individuals; or
- In response to violations of university policies (such as the IT001EN Data Security and Acceptable Use of Information Technology Resources policies); or
- Changes in employment responsibilities upon which access is no longer required; or
- Upon termination of an individual's active affiliation with the university (e.g., employment termination, retirement, graduation, end of vendor contract, death, etc.).

Access to administrative data will be revoked on or before the date of employee termination specified by Human Resources unless an appropriate future job contract has been loaded into the relevant administrative data systems. An exception to the removal of access may be granted to conduct university business for reasons such as, but not limited to coursework, grading, grade appeals, and research activities. Data Security Officers are responsible for documenting exceptions to the removal of access to administrative data. Termination of access to other university IT systems is outlined on the ITS web site.

Individuals with an active university affiliation may request access to data on a "need to know" basis. A Data Security Officer will review the request and may grant access for a specified period. Frequently, the data thus accessed can be downloaded or exported to other applications. All individuals who are granted access to university data are thereby obliged to treat the data according to the same security and privacy rules governing the system of origination regardless of its storage location.

Copies of official data are not authoritative and are therefore not official. Data derived from copies or downloads shall not be used as substitutes for official records kept by the authorized data steward of the university. However, such information may be used to generate official reports on behalf of the university with the knowledge and permission of the official data steward. Such files and resulting reports are covered by the same constraints of confidentiality and privacy as the official records and must be protected according to the applicable data classification standard as defined in University Policy IT0002EN, Information Security Policy.

3.2 Classification

According to University Policy IT002EN, Information Security Policy, restricted University data must be protected against physical theft or loss, electronic invasion, or unintentional exposure through a variety of personal and technical means.

In accordance with this policy, when classifying University data, the following criteria for individual data elements, applications or systems must be used. If there is a question about which category data falls under, always assume the highest possible category in classifying the data.

	Restricted Data	**Internal / Limited Data**	**Public Data**
Definition	Data protected by federal or state law or regulations, or by contract. Restricted University data includes, but is not limited to, data that is protected by the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), (PCI-DSS), General Data Protection Regulation (GDPR), or the Gramm-Leach Bliley Act (GLBA).	Data that would not expose the University to loss if disclosed but should be protected. Internal/Limited access University data includes, but is not limited to, operational data likely to be distributed across organizational units within the University.	Data available within the University community and to the public.
Risk	High	Medium	Low

Access	Individuals designated with approved access.	AUP employees and non-employees with a business “need to know”	AUP affiliates and public with a “need to know”

3.5 Principles for Protecting Data (GDPR)

The six principles of data protection in GDPR are that data must be treated in a way that is:

1. Lawful, fair, and transparent
There must be legitimate grounds for collecting the data and it must not have a negative effect on the person or be used in a way they wouldn’t expect.

2. Limited for its purpose
Data should be collected for specified and explicit purposes and not used in a way someone wouldn’t expect.

3. Adequate and necessary
It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected.

4. Accurate
Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.

5. Not kept longer than needed
Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.

6. Integrity and confidentiality
Data should be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing, loss, damage or destruction, and kept safe and secure.

3.6 In the Case of Misuse

For information on the investigation, determination of violation, and sanction, please see IT0001EN Acceptable Use of Information Technology Resources.”

3.7 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.

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

5. DEFINITIONS

AUP, the University
The American University of Paris

Administrative System

A system designed to facilitate organizational efficiency through standardized business processes, storage, and presentation of data (e.g., CAMS).

Data Entry Standards

Conventions for data entry to ensure data integrity and quality by reducing variation.

Data Security Officer

Individuals responsible for granting, modifying, and revoking security access to specific functional area datasets for a specified period and purpose.

Data Steward

University officials and agents of the university who have designated duties for collection, entry, maintenance, and enrichment responsibilities for data quality and integrity for their functional area.

Data Warehouse

A database designed for analytical and information processing. A read-only collection of data intended to answer business questions.

Database

A structured collection of information, which includes not only data housed in MS SQL or MS Access but also MS Excel, marked-up text files (e.g., xml), and other products used to store data in a structure.

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, Internal / Limited
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.

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.

ITS
Department of Information Technology Services at AUP

Official University Data

Data necessary to the success of the university, whether contained in an administrative system or other university system and considered authoritative.

System

A collection of programs, services, or infrastructure hardware designed to provide specific functionality with regards to supporting university operations and/or data processing activities. Examples include, but are not limited to, email, calendar, file storage, report archive (e.g., academic year census files), reporting (e.g., PowerBI), learning management or course management systems (e.g., Blackboard), administrative systems (e.g., CAMS), and document imaging resources.

User
A person expressly authorized to use University information technology resources and associated services provided by AUP.

NetID
A unique identifier for each user that permits authorization and access to AUP computer resources when used with the correct password.

Violations

Violations of this policy may lead to disciplinary action by the university up to and including dismissal from the university. Under certain circumstances, such violations may give rise to civil and/or criminal liability.

4. APPROVALS & HISTORY

- Approved by the Leadership Team on XX-XX-2022.

5. ISSUING OFFICE AND CONTACT

Chief Information Officer
Information Technology Services
2 bis, Passage Landrieu
75007 Paris
+33 1 40 62 06 96
helpdesk@aup.edu