The American University of Paris

INFORMATION SECURITY

Policy Number: IT002EN
Last Review: 1 February 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. The university provides these resources to support the academic and administrative functions of the institution, and it expects the responsible use of the same.

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. Additionally, the University is committed to protecting its data against threats such as malicious misuse, unauthorized intrusions, and inadvertent compromise. Every AUP department and employee is responsible for the integrity and security of university data used, controlled, or accessed within their area. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities. This policy establishes parameters for the protection of university data.

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 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.

The American University of Paris collects and maintains restricted data about students, employees, donors, vendors, and other parties. This policy governs the use, control and access to restricted data defined by statute, regulation, contract, license, or definitions within this policy. The Data Classification table of IT005EN, the Data Resources, Access, and Usage Policy differentiates the types of university data and establishes guidelines for understanding restrictions.

3.1 Basic Security

Protecting data and information security begins with familiarity with the ITS Information Security web page. The ITS Security web page should be reviewed at the beginning of each academic semester by all account holders. Also, because threats emerge with little notice, ITS will keep news and updates, including measures for threat mitigation, on the web page.

Basic measures for protecting data and information include:

1. Security awareness
2. Access management. Please see IT005EN for Data Resources, Access, and Usage and IT006EN for Data Governance.
3. Password management. Please see IT004EN Password Management and IT001EN Information Technology Resources Rights, Privileges, and Acceptable Use.
4. Multi-factor authentication (MFA). Multi-factor authentication is required for all account holders prior to accessing university computer resources unless an exception is granted by the CIO.

3.2 Security Organization

In coordination with University Leadership and the CIO, the Data Governance Committee (DGC) is responsible for maintaining appropriate procedures for compliance with this policy and providing education to the university community on the implementation of this policy and such procedures. Procedures, technology standards, and best practices can be found at the ITS Security web page.

3.3 Guidelines for Data Storage

University data must be saved to an appropriate location based on the data classification except for rare exceptions approved by the Data Governance Committee. Data stewards may request to store unencrypted restricted data through the CIO's office, and the request will be forwarded to the DGC for approval. The request acceptance or denial will be noted in the minutes of the DGC meeting following the discussion.

If DGC grants permission for university data to be saved and stored on university-owned equipment, personal equipment or cloud-based services, faculty and staff are personally responsible for encrypting the data with the current ITS standards and for remembering the encryption keys or passwords. Users accessing saved and stored university data while on campus must access the data through the university's network.

Restricted university data must be protected against physical theft or loss, electronic invasion, or unintentional exposure through a variety of personal and technical means.

Prior to use of restricted university data via laptop computer or other portable storage media, employees are responsible for obtaining appropriate protections for such computers or portable devices, or for verifying that such protections are already in place. The use of unprotected equipment to access or store university data is prohibited, whether the equipment is owned or controlled by the university or not, unless an exception has been granted by the CIO.

All university computers must have recommended operating system patches and updates installed, updated firmware, updated antivirus and antispyware tools installed, and firewalls turned on. Other devices connected to the university's network must utilize appropriate security protections to the extent possible, including updated firmware.

ITS is responsible for the security of all enterprise information systems of the university, including but not limited to administrative systems, learning management systems, library systems, the central directory system (Active Directory), and Microsoft 365.

ITS will audit systems, servers, computers and portable devices or media for compliance with policies and standards and will deny network access for servers, computers and portable devices or media out of compliance with current best practices.

Remote Access

Remote access to restricted university data is available only to authorized employees. Employees must be authenticated to access restricted university data remotely. Data must be encrypted during transit.

Remote access to university systems is available using approved methods. See the ITS web site for current approved methods.

Personal Computers

Personal computers that are used to access, store, or transmit restricted university data should use current security patches, encryption and updated antivirus and antispyware software. In instances where standard security precautions are not free, the employee will incur all costs for security of their personal computer.

Employees are responsible for deleting all restricted university data from their personal computer upon termination of employment or change in employment when access to the data is no longer required to complete job duties.

Portable Devices, Media, and Cloud-Based Services

Each user in the possession of restricted university data is responsible for protecting the data, regardless of the media or location where the data resides.

Restricted university data may not be stored on any portable device, media, or cloud-based service unless protective measures are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss. Protective measures must be implemented before restricted university data is stored on portable devices, media, or cloud-based service.

Restricted university data stored on portable devices or media must be encrypted with the university's data encryption standard (see the ITS security web page for the current standard). Cloud-based services shall include encryption protection through appropriate, documented business agreements. Documented agreements, including SOC letters and contracts will be stored in a repository.

Equipment Disposal

University-owned computers, portable devices and media must have university data securely erased prior to its transfer out of university control, and/or destroyed, using current best practices. Lost or stolen equipment storing restricted university data must be reported as a Security Incident.

The Information Security web page should be reviewed at the beginning of each academic semester by all users and updated once per term except when new threats require more frequent updates.

3.4 In the Case of Misuse

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

3.5 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 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.

The Data Governance Committee (DGC) is responsible for communicating current security standards and procedures to the university community. These standards and procedures are posted on the ITS Security web page.

Department heads are responsible for ensuring their employees have adequate technical support to understand and implement security standards and procedures. This responsibility extends to data regardless of the storage medium or originating point of access including, but not limited to, university-owned equipment, personally owned equipment, and cloud-based services. Each unit of the university instructs employees about the designated and storage space for saved university data. In the event of an audit, each unit of the university would be responsible for providing the location of the unit's designated and approved storage.

Employees, in cooperation with their Data Stewards, are responsible for protecting restricted university data to which they have access. Employees are required to complete the annual DGC security awareness training.

Employees are responsible for ensuring that appropriate security controls, in accordance with published university standards, are in place to protect restricted university data. This responsibility extends to data regardless of storage media or originating point of access including, but not limited to, university-owned equipment, personally owned equipment, and cloud-based services.

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).

Cloud-Based Service

A vendor-provided service including, but not limited to, storage, analytics, business intelligence, reporting, or other processing, that is not typically located within the university's physical premises.

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.

Encryption

Programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key. Transforming information using a secret key so that the information is unintelligible to unauthorized parties.

Multi-Factor Authentication

Multi-factor authentication (MFA) requires more than one way for people to identify themselves when logging into systems.

Network

Any number of computers and portable devices joined together by a physical or wireless communications link that allows information to be passed between computers, irrespective of where those computers are located. Networks provide the pathways for information traffic and allow employees to access databases and share applications residing on servers.

Official University Data

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

Personal Identifiable Information (PII)

Data that can be used to uniquely identify an individual.

Portable Devices or Media

Portable devices include laptops, Personal Digital Assistants (PDA), cell phones, tablets, or any other portable technology hardware. Media includes technology storage mediums such as CDs, DVDs, magnetic tapes, floppy disks, external hard drives, flash drives and universal serial bus (USB) drives or any other portable storage media.

Public University Data

Data available within the university community and to the public.

Restricted University Data

Data protected by legal or regulatory controls 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), the Gramm-Leach Bliley Act (GLBA), and General Data Protection Regulation (GDPR).

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.

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...

6. APPROVALS & HISTORY

- Approved by the Leadership Team on 02-07-2023.

7. 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