The American
University of Paris

INFORMATION TECHNOLOGY AND DATA GOVERNANCE

Policy Number: IT006EN
Last Review: 1 February 2023

1. PURPOSE

The purpose of this document is to provide the terms of reference and structure for information technology and data governance (hereafter “IT and Data Governance”) at the American University of Paris (AUP). This framework provides a common basis for working with institutional data as a mission-critical university resource. It describes the lifecycle of data and information and the systems, products, projects, processes, policies, and responsibilities that relate to that lifecycle.

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’s most valuable strategic resource is its data. Unlike personnel or money, data can never be replaced if lost or corrupted. Insurance can cover only the financial damage of data loss but cannot restore the institution to its status before the loss. AUP owns and manages vast volumes and varieties of invaluable data related to student and personnel, research, finances, and operations. To safeguard the existence, quality, integrity, and value of its data, AUP maintains a governance framework. This governance framework provides counsel to the systems, products, projects, processes, policies, and responsibilities that support data and information assets. IT and Data Governance provides the means to support the proper valuation, definition, risk management, compliance management, and lifecycle management of the data and information.

IT and Data Governance plays a central role in the control and distribution of important information within the university, ensuing that:

- Decisions about data are made cross-functionally and collaboratively;
- The products, projects, and changes related to the creation and management of data are selected and prioritized cross-functionally and collaboratively;
- Authorization to access, create, update, and delete data is systematic, consistent, and appropriate;
- Data and information are reliable, accurate, and relevant to decision-making;
- The systems and processes are adequate to maintain the best and most appropriate data and information the university needs;
- The university complies with the legal and regulatory requirements for securing the data and information, digital or analog, whether raw, derived, summarized, or aggregated.

In the university context, effective IT and Data Governance will:

- Support the university's strategy to incorporate information technology as an integral part of decision-making, competitive positioning, and service delivery;
- Provide an integrated view, both systemic and detailed, of the functions of the university;

- Prioritize the selection of IT and data products, projects, and changes to provide the maximum value to the university;
- Ensure establishment, maintenance, and delivery of secure, confidential, ethical, trustworthy, stable, reliable, and available collections of institutional data and information;
- Establish and enforce the mechanics for authorization of access;
- Resolve questions of authority or "system of record";
- Improve the value received from technology, data, and information assets by increasing the understanding and appropriate use of the same;
- Improve direct access to data by end-users in accordance with institutional policies, ethical and privacy norms, national, and US and EU privacy and security laws and regulations;
- Establish decision rights with respect to university data that ensure accountability; and,
- Support the university's primary missions of teaching and learning, research, and public service.

3.1 Data Governance Principles

- AUP is the owner of all institutional data and will manage this data as a strategic asset.
- Data quality is defined and monitored to ensure all AUP data are trustworthy.
- For each AUP data element, there is a single system of record and unnecessary duplication of data across multiple information systems will be avoided and corrected where it may exist.
- Institutional data must be stored in a secure manner. Access is provided to internal authorized users who have a legitimate need for data based on their professional role at AUP (Please see IT001EN for Data Resources, Access, and Usage).
- Data are used only for the purposes for which use is authorized and authorization for access to data is not transferable.
- There is a common vocabulary and definition in a data dictionary to describe each data element and data relationship. All metadata are stored and maintained in a shared repository.
- Decisions about data ownership, access, quality, official system of record, and conflict resolution follows consistent processes and is supported by the organizational structure.
- Management of data complies with legal and government requirements, AUP policies, privacy compliance, contractual obligations, and industry best practices.
- All AUP data users uphold the quality and integrity of the data they access, follow AUP's data governance processes, and guard against making incorrect interpretations of data.
- All stakeholders in the data governance process collaborate, cooperate, and coordinate their activities with other AUP departments and programs whose mandate intersects with the management of information systems.

3.2 Data Governance Processes

A. Grant and Maintain Access to Data

Users may be assigned access or may request access to AUP data for purposes of administrative function, systems integration, research and/or external data needs that are consistent with AUP's mandate. Data are overseen by Data Security Officers within each functional area. All requests for data access will be reviewed on factors such as privacy, security, administrative burden, and alignment with AUP values and priorities. If a user is granted access to AUP data, the user will be required to agree to comply with AUP-defined terms and conditions (Please see IT005EN for Data Resources, Access, and Usage and IT002EN Information Security).

B. Define and Maintain Data Quality

Data quality refers to the degree to which data are accurate, complete, timely, and consistent with all requirements and business rules, for a given use. If a user has identified a data quality issue within an enterprise system, the Data Steward within their area will work with the user to triage the issue and define next steps for resolution.

C. Define and Maintain the Data Glossary

A collection of frequently encountered terms in the form of words, vocabularies, phrases, synonyms, acronyms, and codes. Students, faculty, and staff adopting the use of university terms, will be able to communicate and interact more accurately with meaningful concepts in a commonly understood language. Data Stewards will review the AUP data glossary prior to requesting or proposing changes to an existing term or adding a new term.

D. Use and Maintain Data Dictionaries

Software vendors should provide AUP with data dictionaries that support their application software. AUP will need to populate and maintain those dictionaries as they proceed with implementation. Where vendors do not have a data dictionary, the Data Governance Committee will work to define the information for the data dictionary.

E. Define and Maintain Data Standards

Data standards include rules for describing and recording data. They can assert how a field must be populated, rules governing the relationship between fields, and detailed documentation of acceptable and unacceptable values and formats. Data standards are drafted with input from stakeholders and Data Stewards and require approval from the Data Governance Committee.

F. Define and Maintain Reference Data

Reference data is a collection of data that is used solely to categorize, classify, or otherwise qualify or constrain institutional data. It serves as a standard set of codes, values, words, or phrases to be leveraged in AUP’s operational transactions, external compliance, and enterprise reporting and analytics. Use of standardized reference data elevates data quality, and in turn, supports reliable data-informed decisions though consistent data and reporting.

G. Create and Maintain the AUP Data Model

The AUP data model describes the data requirements of the University, and the relationships between them. The purpose of the data model is to facilitate accurate and efficient communication and understanding about the structure, content, and context of institution data to enable data integration and sharing, reporting, and business processes. This model is maintained by the Data Stewards.

H. Identify the System of Record for Data Elements

AUP will need to identify the Systems of Record (e.g., SIS, HR, Finance) for data elements. The Data Stewards will have responsibility for identifying the System of Record for AUP data which will have implications for defining the levels of data access. The system of record is a trusted data source that gives a complete picture of the data object.

3.3 IT Product Selection

All enterprise software products will be submitted for consideration via the software request form of the Help Desk system. The form requires the requester to specify the purpose of the product, the resources required and available to support the initial and recurring cost, timing and timeline considerations, and the executive sponsorship of a Leadership Team member.

The committee will assess the impact of the selection on the Project Roadmap (See below) and the information system, avoiding where possible the duplication of functionality and expense. If the proposal succeeds, the committee will work on a location on the Project Roadmap. If the proposal fails, the decision can be proposed again with changes. If the proposal fails on resubmission, the rejection can be appealed to the Leadership Team with the documented decision and rationale of the Data Governance Committee.

3.4 Project Roadmap

The committee maintains the IT Project Roadmap, which designates the projected start and completion of projects for the coming three quarters. The projects on the roadmap are assigned financial costs, value, timeline, and personnel impact. The Roadmap guides the major projects of ITS and its internal customers and is available on the ITS project web site.

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 07-02-2023.

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