Document title: **AUC Data Governance**

Approval date**: March 2017**

Purpose of document:
The Data Governance Policy manages the quality, consistency, usability, security, accessibility, and availability of administrative data. It covers staff, policies, processes, best practices, awareness and technologies required to manage the university's administrative data. The main objectives of Data Governance include defining data owners, roles, responsibilities and accountabilities, enforcing conformance to data policies, standards, and procedures and resolving data related issues.

Office/department responsible**: The Data Analytics and Institutional Research Office (DAIR)**

Approved by: **Dr. Sherif Kamel, Vice President for Information Management**

Classification level: **Public**

Document accessible: **http://www.aucegypt.edu/about/university-policies**

Document includes:
Data Governance Policy
Appendix A: Data Management Roles and Responsibilities
Appendix B: List of Sample Data Sources
Appendix C: Training and Development

Data Governance

Policy Statement

Data Governance manages the quality, consistency, usability, security, accessibility, and availability of administrative data. This governance covers staff, policies, processes, best practices, awareness and technologies required to manage the university's administrative data as an institutional asset, and focuses on university administrative data maintained by administrative and academic offices.

Reason for Policy/Purpose

The main objectives of the University Data Governance Policy include:

1. To define data owners, roles, responsibilities and accountabilities.
2. To define, approve, and communicate data strategies, policies, standards, procedures, and metrics.
3. To track and enforce conformance to data policies, standards, and procedures.
4. To manage and resolve data related issues.
5. To understand and promote the value of data assets.
6. To reduce university risk by maintaining quality data.

Who Approved This Policy

Dr. Sherif Kamel, Vice President for Information Management Document, March 2017

Who Needs to Know This Policy

Entire AUC community.

Web Address for this Policy

Please list the location on the university's website where this policy is located.

Contacts

Responsible University Official:

Responsible University Office: **The Data Analytics and Institutional Research Office (DAIR)**

If you have any questions on the policy or procedure about Data Governance Policy, you may:

1. Call Rasha Radwan at 26152231, or

2. Send an e-mail to rasha_r@aucegypt.edu

The American University in Cairo
Data Governance

INTRODUCTION

The American University in Cairo administrative data is a mission critical institutional asset that must be adequately used in support of evidence-based decision-making. The office of Data Analytics and Institutional Research (DAIR) is the focal point for administering, supporting, and promoting this activity. Data Governance manages the quality, consistency, usability, security, accessibility, and availability of administrative data. This governance covers staff, policies, processes, best practices, awareness and technologies required to manage the university's administrative data as an institutional asset, and focuses on university administrative data maintained by administrative and academic offices.

OBJECTIVES

The main objectives of the University Data Governance Policy include:

1. To define data owners, roles, responsibilities and accountabilities.
2. To define, approve, and communicate data strategies, policies, standards, procedures, and metrics.
3. To track and enforce conformance to data policies, standards, and procedures.
4. To manage and resolve data related issues.
5. To understand and promote the value of data assets.
6. To reduce university risk by maintaining quality data.

Data Management Policy

POLICY

This policy is concerned with University Administrative Data. Such data is owned by The American University in Cairo. All members of the University community are responsible for appropriately and objectively using, as well as safeguarding such data. This policy establishes uniform data management standards for Administrative Data, and identifies the shared responsibilities for assuring the following:

1. The integrity of Administrative Data.
2. That Administrative Data efficiently and effectively serve the needs of the University.
3. The presence of, and conformance to a uniform set of definitions for commonly used data across the university, wherever applicable.
4. Confidentiality and privacy of Administrative Data.
5. Meeting compliance and regulatory requirements.
6. The reporting of actual or suspected cases of breach of information security (confidentiality, integrity, or availability), to the office of Information Security for due handling.

This policy shall be reviewed on an annual basis. It is owned by the office of Data Analytics and Institutional Research.

SCOPE OF THE POLICY

This policy applies to:

1. All employees, supervisors and managers whose job responsibilities include updating, safeguarding, extracting, or usage of Administrative Data.
2. The University as a whole including but not limited to, all of its campuses, schools, units, centers and administrative departments.
3. All Administrative Data of all kind regardless of means or location of storage. This policy applies to Source Data Systems and Administrative Data extracted from those Source Data Systems, as well as data stored in any data repository.

Individuals affected by this policy include all data management roles of institutional data, information and knowledge including, but not limited to, the list available in Appendix B.

A. GUIDING PRINCIPLES

1. The Office of Data Analytics and Institutional Research (DAIR) is responsible for promoting and enforcing this policy, in collaboration with other offices on an as-needed basis. The office of Information Security of the University is responsible for proactively coordinating with DAIR with regards to all aspects of Information Security pertaining to this governance document.
2. In order for the University to effectively manage and safeguard its Administrative Data, procedures must be in place to guide its appropriate access, to ensure its security, and to provide a means to address procedural exceptions. It is necessary for all employees who deal with Administrative Data to be trained and informed about data security.
3. Role definitions of individuals with data responsibilities are necessary to support data integrity and security.
4. Sharing Administrative Data within the University should be facilitated where appropriate, subject to appropriate security restrictions as established by each Data Domain Trustee and ratified by the Data Trustees.
5. Implementation of this policy will reinforce a uniform set of definitions for commonly used

data across the university when possible (e.g., "enrolled student" should have the same meaning throughout the University).

6. Integration of Administrative Data across the University should be encouraged to foster data accuracy and uniformity. This should result in reduced duplication of data and greater data accuracy.
7. Administrative Data should be safeguarded to maintain the confidentiality and privacy of personally identified information.

B. DATA ADMINISTRATION

1. University Ownership of Administrative Data

All Administrative Data is owned by The American University in Cairo. As such, all members of the University have the obligation to appropriately use and safeguard the asset, in all formats and in all locations.

2. Stewardship

Roles and responsibilities for safeguarding and classifying the Administrative Data asset are defined below in section C, Data Management Roles and Responsibilities.

3. Information Classification

Administrative Data is categorized and retained as per the University related policy.

4. Access, Security and Confidentiality

a) Access to institutional data is granted internally based on an institutional need-to-know-basis to support institutional decision-making. Employees are granted access to institutional data needed to perform their duties by virtue of their position at the University. Authorization for access to data is not transferable. Access to data is granted only after a Confidentiality Agreement is signed by the person obtaining access.
b) Proper, business friendly and accepted secure access tools and mediums must be in place and deployed regardless of the data representation form, these tools and mediums need to be approved by both the Data Steward and the office of Information Security.
c) Data Disposal mechanisms need to be executed securely as well as Data mediums disposal (Example: Hard Disks, Servers…etc.) as per the agreement of the relevant Data Steward, Data Custodian and the office of Information Security.
d) Data Domain Trustees, Internal Auditor, Legal Affairs, the office of Information Security and the office of DAIR reserve the right to audit and review activities of all users and administrators of any Data Source system.
e) In case of any access violation, intentional record tampering, breach of confidentiality, or similar suspicious activities whether actual or suspected, such incidents must be reported to the office of Information Security for due handling.
f) Data Trustees are responsible for granting access to Institutional Data, defining and implementing the standard procedures for requesting and approving access to Institutional Data irrespective of the type of the data. All procedures should include adequate tracking for requests and approvals such that authorized access to Institutional Data is auditable.
g) For information that is not accessible to the requesting user as per the University Information Classification Policy, granting access is contingent on the signature of a standardized Confidentiality Agreement for all users at all levels of the institution. Data custodians are responsible for enforcing this process. The office of Data Analytics and Institutional Research (DAIR) will make available a Confidentiality Agreement for such purposes (in collaboration with relevant offices of the University).
h) The office of Data Analytics and Institutional Research (DAIR) has the right to inquire and request access to all sorts and forms of institutional data. DAIR has the right to all operations related to institutional data, data standards, data definitions and governance; inquire, extract, collect, analyze, disseminate, report, quality check and disclose data. In case the access requires signing a Confidentiality Agreement, the same requirements applicable to data Stewards should

be extended to DAIR staff and systems. Upon formally requesting inquiry about, or access to data, the office of Data Analytics and Institutional Research (DAIR) must obtain access to their requested data, or response to their inquiry within two business days from the initiation of the formal request. In the case where DAIR is unable to have their request fulfilled within reasonable time beyond the two business days, DAIR has the right to arbitrate the case with the VP/Chief Digital Officer (or equivalent role), who will have final decision as relates to the request being made, or arbitration will be done including the corresponding area head along with the responsible senior administrator at the University cabinet level.

i) Institutional data must be stored in such a way as to ensure that the data is secure, and covered by a Disaster Recovery Plan developed and/or approved by the office of Information Security and other concerned units. Data custodians must ensure that passwords and other security mechanisms are used, and that access is limited to authorized users.
j) Users are responsible for protecting the data they have access to against making misinformed or incorrect interpretations of data or misrepresentations of information. Data users must not knowingly falsify, delete or change data without providing sufficient justification and securing necessary approvals.
k) *Access* to institutional data is granted externally when release of such data would not violate the university's policies. External access should be governed by contractual agreement and approved by the University Legal Advisor and the VP/Chief Digital Officer (or equivalent role). External users should sign a Confidentiality Agreement.
l) The University office of Information Security is responsible for working closely with the various stakeholders to promote security expectations listed herein this document.

In order that the proper controls are applied, it is the responsibility of each person accessing Administrative Data to: (a) know the classification of the system being used, (b) know the type of Administrative Data being used, (c) follow the appropriate security measures, and (d) consult the related policies for further information. It is their right to also be duly trained with respect to aspects listed herein.

5. Training

Before an individual is permitted access to Administrative Data in any form, training on the use and attributes of the data, functional area data policies, and University policies regarding data is required. For users with current access, and who have not received prior training, DAIR will communicate the need, and scope of training to relevant offices of the University. The Data Domain Trustees shall establish the appropriate levels of training for all such individuals within their units. The training will be recurrent based on needs and requirements. DAIR will coordinate regular data governance awareness campaigns to the University community.

6. Integrity, Validation, and Correction

Administrative Data must be safeguarded and managed in all formats and media (e.g., print and digital), at all points of access, and across all University systems through coordinated efforts and shared responsibilities. Each Data Trustee, in conjunction with the appropriate Data Domain Trustee, shall be responsible for developing a plan for their functional area to assess the risk of erroneous or inconsistent data and indicate how such Administrative Data, if found, will be corrected. The office of Data Analytics and Institutional Research (DAIR) will be responsible for ensuring that each functional area develops a plan according to expectation, and uses that plan to develop and implement processes for identifying and correcting erroneous or inconsistent data. Disputes between DAIR and any other University office with respect to planning will be reported to the VP/Chief Digital Officer (or equivalent role) for arbitration, and for the appropriate decision to be taken.

7. Extraction, Manipulation, and Reporting

Extraction, manipulation, and reporting of Administrative Data must be done only for University business purposes, or subject to terms of use as otherwise approved by the Data Trustee Committee. Personal use of Administrative Data, in any format and at any location, is prohibited except with

the prior written approval of DAIR. The office of Data Analytics and Institutional Research (DAIR) is the sole entity responsible for official reporting of institutional data, information, knowledge or analytics needed for institutional decision making. Where data extracted or reported cannot be reconciled with the official institutional data, it cannot be considered official institutional data or presented as such. All units reserve the right to extract and analyze operational information to serve their business needs. Any representation of the data or information in the form of reports, web pages, paper documents, other forms will include a disclaimer that indicates that the data or information are not official institutional data.

C. DATA MANAGEMENT ROLES AND RESPONSIBILITIES

Data management roles with responsibilities are outlined below. Refer to Appendix A for specific details.

1. Data Trustee

Data Trustees are senior University officials (typically at the level of Vice President, Provost or higher) who have planning and policy-making responsibilities for Administrative Data and for the establishment of operational processes to collect and record data in accordance with University business rules. The Data Trustees, as a group, are responsible for overseeing the establishment of Administrative Data management policies and procedures, and for the assignment of data management accountability.

- Oversee the establishment of data management policies and processes.
- Assign Data Stewards and Data Domain Trustees.
- Serve as an escalation point for problem/policy resolution.
- Approve the Business Continuity and Disaster recovery deliverables (Example: maximum data loss in case of disasters and maximum tolerable time without data availability…etc.).
- Approve record retention and archiving guidelines in accordance with the University business needs and legal regulations.
- Authorize Data change hold in case of legal/audit related data freeze requests.

2. Data Domain Trustee

Data Domain Trustees are senior managers in operational areas responsible for maintaining the content of Transactional Systems. The Data Domain Trustees implement policy as established by Data Trustees, assign Data Stewards, and serve as the first escalation point for problem/policy resolution from the Data Stewards.

3. Data Steward

Data Stewards are typically operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the Transactional Systems. Data Stewards are appointed by the respective Data Domain Trustees.

- Certify data deposited in the warehouse.
- Certify standard reports and dashboards.
- Oversee the resolution of data errors.
- Participate in establishing common definitions.
- Assist in collecting and recording metadata.
- Establish and manage policy for record retention and archiving.
- Suggest and implement proper security controls.

4. Data User

Data Users are individuals who access Administrative Data to perform their assigned duties. Data Users are responsible for safeguarding their access privileges, for the use of the Administrative

Data in conformity with all applicable University policies, and for securing such data.

5. Data Custodian

The Data Custodians are information technology staff assigned to each ERP system which maintains Administrative Data. Data Custodians oversee the safe transport and storage of data, establish and maintain the source data systems, and perform activities required to keep the data intact and available to users.

In addition, Data Custodians are responsible for working with Data Stewards and the office of Data Analytics and Institutional Research (DAIR) to develop automated processes which identify erroneous, inconsistent, or missing data and resolve data issues. Their responsibilities include:

- Establishing and maintaining the underlying source data systems.
- Ensuring the accurate transfer of data into the University Data Warehouse using automated validation and error management processes.
- Performing activities required to keep the data intact and available to users.
- Collaborating with the Decision Support Group and the Data Stewards to implement data transformations, resolve data issues, and manage system changes.
- Developing the data governance infrastructure strategy, including policies, roles, responsibilities and processes.
- Works with Information Security to establish proper security controls.

6. Office of Data Analytics and Institutional Research (DAIR)

The office of Data Analytics and Institutional Research is responsible for data, information or knowledge used in official reporting. This includes, but is not limited to, generate all official institutional reporting of data, information, knowledge and analytics, to internal and external entities on behalf of the University, working with the appropriate Data Stewards to develop standard definitions of commonly used terms; define how official University metrics are calculated; work to discover data discrepancies, inconsistencies and gaps and will promptly report such to the appropriate Data Steward for resolution.

7. Council for Information Management (CIM)

The University Council of Information Management is the focal point for discussion and decision support for all aspects of information and information technology governance within the business ecosystem of the university. The Council for Information Management (CIM) establishes overall policies for management and access to the Administrative Data of the University. This council shall provide oversight of all University processes which capture, maintain, and report on Administrative Data. The Council shall be made aware of activities related to the creation and maintenance of such processes, and reserves the right to review them on an as-needed basis".

8. Office of Information Security

The office of Information Security is responsible for all technical access and security logs, audit trails, authentication logs, traffic flows evidence, data access evidence, etc. for all AUC digital services and Data sources. The office is also responsible for related security based analysis, evidence collection, correlation and reporting. The office of Information Security works with Data Stewards and Data Custodians to ensure that proper security controls, change audit logs, secure access procedures are in place. This office will proactively work with relevant entities to promote and enforce its reasonable expectations regarding Information Security.

Appendix A: Data Management Roles and Responsibilities

Data Type	Data Trustee	Data Domain Trustee	Data Steward	Reporting
Students Recruitment Data	The Provost	Associate Provost for Strategic Enrollment Management	Chief Enrollment Officer	DAIR
Students Admission Data (Undergraduate)	The Provost	Associate Provost for Strategic Enrollment Management	Chief Enrollment Officer	DAIR
Students Registration Data	The Provost	Associate Provost for Strategic Enrollment Management	University Registrar	DAIR
Students Financial Affairs Data	EVP For Administration & Finance	University Financial Controller	Director Student Accounting	DAIR
Students Financial Aid Data	EVP For Administration & Finance	Executive Director, Office of Student Financial Affairs and Scholarships		DAIR
Students Admission Data (Graduate)	The Provost	Dean of Graduate Studies	Director of Graduate Admissions	DAIR
Students Graduate Fellowships	The Provost	Dean of Graduate Studies		DAIR
Students Athletics Data	EVP For Administration & Finance	AVP for Campus Services	Athletics Director	DAIR
Students Activities Data	The Provost	Dean of Students	Director of Student Engagement	DAIR
International Students	The Provost	Associate Provost for Strategic Enrollment Management	Director of International Programs Office (IPO)	DAIR
International Students	The Provost	Dean of Students	Director of International Student Life (ISL)	DAIR
Student Library Records	The Provost	Dean of Libraries and Learning Technologies	Director of Library Automation Systems	DAIR
Student Housing	EVP For Administration & Finance	AVP for Campus Services	Director, Office of Residential Life	DAIR
School of Continued Education Data	Provost	Dean of School of Continued Education	Exec. Director, Strategic Management	DAIR
Course Catalog, Schedule, Faculty Assignment	The Provost	Associate Provost for Strategic Enrollment Management	University Registrar	DAIR
Full Time Faculty Data	The Provost	The Provost	Assistant Provost for Faculty Affairs	DAIR
Part Time Faculty	EVP For Administration & Finance	Executive Director for Human Resources	Senior Manager, Faculty Affairs	DAIR
Faculty Housing	EVP For Administration & Finance	AVP for Campus Services	Sr. Dir, Faculty Housing & Transport. Services.	DAIR
Staff	EVP For Administration & Finance	Executive Director for Human Resources	Director, Staff Affairs	DAIR
External Research Data	The Provost	Vice Provost	Director, Office of Sponsored Programs	DAIR
Internal Research Data	The Provost	Vice Provost	Senior Officer - Office of the Vice Provost	DAIR
Finance (Budget)	EVP For Administration & Finance	Executive Director, Budget & Financial Planning		DAIR
Finance (Endowment, Financial Statements)	EVP For Administration & Finance	University Financial Controller	Director, Financial Analysis & Reporting	DAIR
Employability	The Provost	Associate Provost for Strategic Enrollment Management	Executive Director, Career Center	DAIR
Energy/Water Consumption	EVP For Administration & Finance	AVP for Campus Services	Sustainability Officer	DAIR
Alumni	VP for Advancement and Communications	Executive Director, Alumni Eng.& Annual Fund		DAIR
Development	VP for Advancement and Communications	Executive Director, Development		DAIR
Communications	VP for Advancement and Communications	Executive Director for Communications		DAIR

Appendix B: List of Sample Data Sources

Student Information System	Banner Student
Administrative System	SAP
Resource Allocation System	AdAstra
Career Services System	Career Web
Research Systems	SciVal
Faculty Systems	eRepertoire
Alumni and Fund Raising Systems	Sales Force
Process and Work Flow Systems	Axiom and Perceptive
Survey Systems and/or any survey related data/sources	
Planning, Assessment and Accreditation Systems	Compliance Assist
Digital Archive and Research Repository	AUC DAR
Rare Books and Special Collections Digital Library	OCLC CONTENTdm System
Archival Description System	ArchiveSpace
Web Archiving System	Archivelt
Library Systems	Sierra
All in house developed systems	Ex: Planning Matrix
All other systems and data sources	

Appendix C: Training and Development

Student Information System	Banner Student	Office of Strategic Academic Services
Administrative System	SAP	HR Module: Office of Human Resources Budget Module: Office of Budget and Financial Planning Supply Chain Module: Office of Supply Chain Management Financial Module: Office of the Controller
Resource Allocation System	AdAstra	Office of University Information Systems
Career Services System	Career Web	Office of Career Services
Research Systems	SciVal	
Faculty Systems	eRepertoire	
Alumni and Fund Raising Systems	Sales Force	Alumni Office
Process and Work Flow Systems	Axiom and Perceptive	Office of University Information Systems
Survey Systems and/or any survey related data/sources		Office of Data Analytic and Institutional Research
Planning, Assessment and Accreditation Systems	Compliance Assist	Office of Data Analytic and Institutional Research
Archiving Systems	AUC DAR, OCLC CONTENTdm, ArchiveSpace, ArchiveIT	Rare Books and Special Collections Library
Library Automation System	Sierra	Library Automation Systems
All in house developed systems	Ex: Planning Matrix	Office of University Academic Computing
All other systems and data sources		

History/Revision Dates

Origination Date: October, 31, 2016
Last Amended Date: March, 10, 2017
Next Review Date: March, 10, 2018