

Information Technology Management Principles, Policies and Guidelines

- Reference:** CNS-P-ADM-APPS **Revision:** A
- Supersedes:** None
- Purpose:** The purpose of this policy is to define the guidelines and standards that govern the management of mission critical business processes, computing systems and administrative applications (ADM-APPS) at the American University of Beirut (AUB).
- Source:** Computing and Networking Services (CNS).
- Approved by:**
- | | |
|--------------------------------------|-----------------------------|
| Nabil Bukhalid, Director of CNS | on: December 4, 2001 |
| George Tomey, VP for Administration | on: Pending |
| Peter Heat, Provost | on: Pending |
| Nadim Cortas, VP for Medical Affairs | on: Pending |
| John Bernson, VP for Finance | on: Pending |
| Steve Jeffrey, VP for Development | on: Pending |
- Applicability:** This policy and guidelines apply to all mission critical administrative computing systems involved with the creation, updating, processing, reporting, distribution, archiving and other uses of administrative information at the American University of Beirut and its Medical Center.
- The guidelines are independent of the system architecture and apply to web-base systems, client/server applications, and server centric applications whether developed in-house, acquired from external vendors or a result of extensions to existing or purchased applications.
- The guidelines apply to all administrative applications that deal with students, patients, financial, administrative, or other business information that is an integral part of running the business of the University and the Medical Center. They apply to any process or application that affects more than one person's job responsibilities.
- Background:** AUB is briskly replacing its legacy administrative computing systems and computerizing new business areas and processes in compliance with market best practice and leading information

systems architecture based on the principles of open standard, web enabled and/or client/server systems and technologies.

The deployment of the new administrative computing systems at the University started in 1998 coinciding with major changes in the management organization, mainly at the executive level.

The concurrent changes and the accompanied change management initiatives did not address in a perceptive manner the impending information technology management principles, institution-wide processes and information systems ownership, interoperability, inter-process dependencies, shortest path optimization, systems' audit and security, common standards, documentation, quality control and quality assurance, etc.

The new administrative computing architecture is expected to sustain and support the University and Medical Center information technology needs for at least ten years. This is a large-scale change that will fundamentally affect the way the University does its business for many years to come.

Policy: **AUB academic and administrative policies and procedures, processes, and supporting information technology are designed to enhance productivity, reduce costs and enable efficient and effective workflows.**

Every institution-wide process has a designated **process sponsor/owner** who is responsible for ensuring the fit of that process to the business needs of its customers.

Every administrative computing system, supporting an institution wide mission critical process or a departmental centric process, has a designated **functional sponsor/owner** who is responsible for ensuring the fit of that system to the processes it supports.

Every administrative computing system, supporting an institution wide mission critical process or based on the sponsor/owner request a departmental centric process, has a designated **IT coordinator** who is responsible for ensuring that the system is consistent with AUB-adopted administrative computing system design, implementation and management standards and procedures., being request for proposal (RFP), request for development (RFD), project management, design and implementation documentation, process and system audit and security, data object definition and custodianship, data backup and retention, interoperability and integration, unique identification, application source escrow assurance and quality

Accountability is assigned for every administrative data object. Roles and responsibilities of data custodians, data maintainers and data users are clearly defined to ensure the quality, security, accessibility, and preservation of AUB administrative data.

Guidelines: **RESPONSIBILITY:** The owner of an administrative system is responsible for the definition of the scope of the project, development of a project plan, assignment of responsibilities, and management of the project.

An administrative system owner who does not use the services of the Computing and Networking Services for design, development, or maintenance of an administrative system must assume both the system owner and the system developer responsibilities.

Operators of distributed computing systems, remote network servers, or small stand alone systems must satisfy all the responsibilities of administrative system owner, developer, user and operator in succession, on an ongoing basis.

Computing and Networking Services will designate an IT coordinator to monitor and quality control any and all institution-wide mission critical administrative system.

a. Process Sponsor/Owner Responsibilities

- Define and document the process workflow.
- Ensure that the process fit the business requirements and functionality.
- Ensure that the process is optimal and delivers quality service to its customers.
- Ensure adequate data object accountability.
- Ensure adequate data collection and validation from the source.
- Ensure that data custodians, data maintainers and data users are clearly assigned, adequately trained and explicitly clear about their roles and responsibilities
- Define the functions, procedures, reports and audit requirements of the administrative system.
- Ensure the request for proposals (RFP) or Request for Development (RFD) and the proposed designs meets the system requirements.
- Ensure adequate controls, audit trails, security, backup, recovery and restart procedures are included in the design.
- Ensure an adequate test plan is prepared and monitor the testing and review of the system during development and/or configuration.
- Define and ensure compliance with system acceptance criteria. Formally accept the system as complete and ready for production

b. System Owner Responsibilities

- Define the functions, procedures, reports and audit requirements of the administrative system.
- Ensure the request for proposals (RFP) or Request for Development (RFD) and the proposed designs meets the system requirements.
- Ensure adequate controls, audit trails, security, backup, recovery and restart procedures are included in the design.
- Ensure an adequate test plan is prepared and monitor the testing and review of the system during development and/or configuration.
- Define and ensure compliance with system acceptance criteria. Formally accept the system as complete and ready for production.
- Ensure an adequate training plan is prepared and delivered to the system users.
- Ensure the design and development of the system meet all appropriate functional standards.
- Provide for the completeness and accuracy of all required user and system documentation for the system.
- Authorize system implementation and all program changes.
- Manage, control and review access to the system and its data. Maintain and review data security and integrity.
- Manage and control user access to the system. Monitor and review user access logs. Define, approve and manage user access permission and authority levels.
- Designate a system operator or administrator responsible for day to day decisions regarding the operation of the system.

c. IT Coordinator Responsibilities

- Review and recommend changes to the functions, procedures, reports and audit requirements of the administrative system.
- Ensure that the appropriate hardware and software environment is selected for the development and operation of the system.
- Review, recommend changes and ensure the request for proposals (RFP) or Request for Development (RFD) and the proposed designs meets AUB standards.
- Review, recommend changes and ensure that adequate controls, audit trails, security, backup, recovery and restart procedures are included in the design.
- Review, recommend changes to the test plan and monitor the testing and review of the system during development and/or configuration.
- Define and ensure compliance with system acceptance criteria. Formally accept the system as complete and ready for production.

- Ensure the design and development of the system meet all appropriate technical standards.
- Review the system documentation for completeness and accuracy.
- Define and ensure compliance with the system installation procedures. Define and monitor procedures for modifying the system. Authorize all program changes.
- Review and approve to the data security and integrity. Review and approve data sharing procedures in order to ensure the integrity of interfacing systems.
- Define and manage quality control and quality assurance procedures for data backup and system security.

d. System Developer/Integrator Responsibilities

- Develop and/or integrate the application to the satisfaction of the administrative system owner, translating the system requirements into design requirements.
- Create a design that provides for functionality and ease of use, or select a product that meets system owner requirements.
- Design, code, install, test and deploy the application in compliance with all appropriate standards.
- Implement the most effective methods of satisfying the control and audit requirements established by the system owner, or resulting from design decisions.
- Implement the most appropriate methods of meeting the system security standards.

e. System User Responsibilities

- Comply with user procedures and security requirements as established by the administrative system owner.
- Comply with all control requirements specified by the administrative system owner.

f. System Operator Responsibilities

- Create a secure operating environment that promotes efficient use, including appropriate procedures to protect and recover data and a secure physical environment.
- Protect against, monitor for, and detect unauthorized access to the system or data files and report to the appropriate security officer.

INVESTMENT CRITERIA: Evaluation and approval of information system investments is based on a business case and full-cost analyses, including the costs of managing and maintaining technology investments throughout their expected useful lives.

Investments in new information technologies are made to improve or sustain business practices or management decision-making in support of the University's mission and vision. They are cost-

effective for the University as a whole, and consistent with the adopted technology standards.

INFORMATION AVAILABILITY: University administrative data is sufficiently accessible, comprehensive, timely, accurate, and flexible to accommodate the information and reporting needs of faculty, doctors, staff, and students. It is made available to all with a legitimate need, consistent with AUB's responsibility to preserve and protect data privacy.

To ensure cross-system interoperability and consistency, reference data and other shared data is made available to individuals and applications from single, authorized source databases that utilize consistent data definitions and business rules.

The technical infrastructure provides students, faculty, doctors and staff with convenient access to institutional and global computing and information resources and facilitates interaction and collaboration among individuals and groups.

DATA COLLECTION and ADMINISTRATION: University systems collect information electronically and directly from the information source, and deliver it electronically and directly to those who need it. Intermediaries are added to the process only if they increase the value to the information being transmitted.

University administrative data is collected and validated once, and is re-validated only when transformed.

AUB follows institution-wide data administration policies and practices to ensure data coordination, integration, and integrity across systems.

INFRASTRUCTURE and CORE SERVICES: AUBnet and CNS data centers technical infrastructure is optimized to support both web and client/server data capture and data access.

The infrastructure provides a common set of core services that supports efficient implementation, operation and management of applications in a distributed and collaborative computing environment.

Core infrastructure services are provided to support access and interoperability between administrative computing systems.

The infrastructure is accompanied by adequate support services to provide reliability, availability, and serviceability to meet AUB business and information needs.

STANDARDS: AUB technical infrastructure conforms to a set of open system standards and supports a limited number of hardware, software, and networking choices.

AUB continually evaluates new technologies, standards, and products that have the potential to further enable AUB's academic mission, lower costs, or improve overall productivity.

APPLICATION DESIGN and IMPLEMENTATION:
Applications are designed and implemented to be easily adaptable to multiple and changing business and technology needs.

Applications are designed and implemented so that data collected and maintained by them may be used for multiple purposes, including operations, planning and decision making.

Application interface designs conform to an AUB user interface standard that ensures consistency of appearance and behavior across applications and platforms.

Consequence of

Non-Compliance: Non-compliance with this policy could severely impact the operation of the institution by exposing the University to permanent loss of university data leading to loss of financial records, students' records, patients' records, research material and/or university and research funds. It may also expose the individual or the University to legal action.

Definitions: **ADMINISTRATIVE COMPUTING SYSTEM:** is the collection of processes, data objects, functions and reports which are relevant to the operations or management of one or more AUB unit.

Additional

Information: - None