

Administrative Application (ADM-APPS) Data Access Policy

- Reference:** CNS-P-ADM-APPS-ACCESS **Revision:** A
- Supersedes:** All XXX-ACCESS Procedure **Effective:** October 2005
- Purpose:** The purpose of this policy is to establish a generic administrative application Data access policy and procedures to be complemented by compliant detailed procedures specific to each administrative application..
- Source:** Computing and Networking Services (CNS).
- Approved by:** Nabil Bukhalid, Director of CNS **on:** October 9, 2005
Peter Heath, Provost **on:**
- Applicability:** All administrative applications the list a few: Student Information System (Banner); Library Information System (OLIB); and Financial Information System (OSCAR).
- Background:** The University is the owner of all administrative data; individual units or departments may have sponsorship/stewardship responsibilities for portions of that data.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to its access, or failure to maintain quality. The University expressly forbids the use of administrative data for anything but the conduct of institutional business. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use. In addition, the University and its employees should comply with applicable incumbent laws and regulations.

The University determines levels of access to administrative data according to principles drawn from various sources. Law and regulations provides in some instance description of some types of information to which access must be restricted. In an academic community, ethical considerations are another important factor in determining access to administrative data.

Policy: Information, data domains and data elements maintained by the University are a vital asset that will be accessible to all employees who have a legitimate need for it, consistent with the University's responsibility to preserve the quality and protect such information by all appropriate means.

- The data security contact in consultation with the data steward and CNS must develop and maintain current a clear “Application Specific Access Procedure” in line with this policy and its recommended procedures.
- The head of the user’s department, and the data security contact for the data domain must authorize access to the system.
- The application form will include both an acceptable use statement and a statement concerning use of the information.
- All accounts will be deleted when an individual leaves AUB or when a person leaves a position that required access to administrative systems.
- User’s accounts must be traceable to individual users leaving no room for repudiation.
- All department heads must re-authorize user access every 12 months.

The quality of data in this context, is a collective characteristic that encompasses utility, objectivity, integrity, accuracy and completeness. Data quality is supported by presentation in an accurate, clear, complete, and unbiased manner, with sources identified in appropriate fashion, with potential sources of error identified, and with disclosure of the degree to which the data has been protected from unauthorized access or revision, from compromise through corruption, and from falsification

A data domain is the entire collection of data for which an institutional employee functioning as a data steward or data security contact is responsible. The data domain also includes rules and processes related to the data.

Access to data is either (a) the capacity for data processors to enter, modify or delete data or (b) the capacity for data users to view, copy or download data.

Procedure: **Timeliness and Business Process Continuity** – The data security contact is responsible for the follow up on access requests pertaining to his/her data domain and the primary database administrator is responsible for the timely execution of such requests. After that the data security contact is responsible for the quality control / quality assurance of the granted access rights.

Deletion of a user’s account or termination of a specific data access should be duly analyzed to secure business process continuity thus providing forwarding instruction to any request addressed to the user that is still in in-progress.

Request for Access to Administrative Application Data:

Application User ID – CNS recommends the use of AUBnet ID whenever possible as this will facilitate user account traceability and management.

Categories of Data - Access to specific categories of data by the University employees or by non-University employees sponsored by a VP or Head of a department requires that a formal request be made to the appropriate data security contact (refer to the Application Specific Access Procedure for current contact details). The request can be via a simple email using appropriate “User Account Request Form”.

Exceptions - All requests for exceptions to data access policies must be made in writing to the data security contact. E-mail requests are acceptable. The request must specify the data desired and their intended use. In addition CNS might request from the requester to complete a Privileged Access Form to be approved by his supervisor and the data security contact for the domain.

Denial - The data security contact must provide a written record of the reasons for denial of any request to access institutional administrative data. E-mail records are acceptable.

Appeal - Members of the institutional community may appeal any decision that denies access to institutional administrative data. Appeals may be made to the appropriate system sponsor/data steward.

Renewal - All department heads must validate user access every 12 months. The data security contact is responsible for the initiation, planning and execution of the validation process.

Request for Deletion of a User Account:

Termination Request Initiated by a Supervisor – Deletion of a user account or termination of access to a specific categories of requires that a formal request be made to the appropriate data security contact by a user’s supervisor. The request can be via a simple email using the appropriate “User Account Request Form”.

Deletion of a User Account Initiated by Employee Clearance Process and/or Change of Status on NetDB – All user accounts will be deleted when an individual leaves AUB or when a person leaves a position that required access to administrative systems. The Clearance System will auto-notify via email the appropriate data security contact.

Definitions: 1. Administrative Data or Institutional Administrative Data

The institutional database consists of information critical to the success of the University as a whole. The institutional database is shared data,

distributed over a number of systems and managed within a conceptual framework. It is likely that the institutional database will be distributed across processing units both within and outside the central IT. Specific types of data, such as research data and electronic mail "boxes," may be covered by specially tailored policies.

Data may be digital text, graphics, images, sound, or video. The University regards data that are maintained in support of a functional unit's operation as part of the institutional administrative database if they meet at least one of the following criteria:

- if at least two administrative operations of the University use the data and consider the data essential;
- if integration of related information requires the data;
- if the University must ensure the quality of the data to comply with legal and administrative requirements for reporting statistical and historical information externally;
- if a broad cross section of institutional employees refers to or maintains the data; or
- if the University needs the data to plan.

Some examples of administrative data include student course grades, patient records, employee salary information, vendor payments, etc.

2. Institutional Administrative Data Categories

[Note: Data Categories are subject to review by the IT Steering Committee]

General administrative data - General administrative data are all data that are not either legally restricted or judged by data stewards to be limited-access data. Any data that are published and broadly available are, of course, general administrative data. University policy holds that the volume of data classified as general administrative data should be as large as possible because widespread availability of such information will enable employees to make creative contributions in pursuit of the University's mission. Examples of digitally published data (a subset of general administrative data) include digital editions of the university statistical reports.

Legally restricted data - Legally restricted data are those data that require restrictions on access under the law or that the University decides to restrict in accordance with internal policies. Public requests for legally restricted data are reviewed by legal counsel prior to responding. Examples of legally restricted records and data are transcripts and education records and they may be provided to the subject student only.

Limited-access data - Some data that are not legally restricted may be designated by University data stewards as data to which access by University employees is limited. Although its release or disclosure may be authorized under law these data are not routinely made available to broad audiences. To access these data, University employees must follow the

procedures developed by the data steward responsible for the data. Criteria for assignment of data to this category are developed by the relevant data steward.

Data stewards might consider the following factors in deciding whether or not to limit viewing, copying and downloading of data:

- Is data administratively sensitive?
- Is data easily misinterpreted?
- Is this data for which the University is owner or steward?
- Does the data have implications for personal safety of employees or students?
- Does the data reveal security information or expose the security of the operation?

3. Roles Related to Institutional Administrative Data

As part of their jobs, University employees take on various roles and responsibilities with respect to institutional administrative data. Under the guidance of various institutional leaders employees may fill the roles of system sponsors/data stewards, data security contacts, data users, and data processors. In addition, various individuals and groups provide data-related services, especially the database administrators and security officer in CNS.

Roles	Responsibilities
System sponsors/ Data stewards	Vice President or department head with primary responsibility and accountability for institution data, including creation and maintenance, within their appropriate data domains. They determine who may create, maintain, and use data in the domain area(s) for which they are responsible, and they are responsible for ensuring the quality of data entered. They are responsible for ensuring that the system for which they serve as sponsor is operable and available to all authorized users.
Data security contacts	Carry out the data domain policies set by the data stewards, as well as the institution's overall administrative data security policies; play major approval role in data access authorization processes.
Data users	View, copy or download data, but do not enter, modify or delete it.
Data processors	Enter, modify, or delete data.
Database Administrators	Develop and apply standards for the management of institutional data and for ensuring that data are accessible to those who need it. They work closely with the data stewards on formulation of domain data policies, standards, and procedures.
Security Officer	Coordinates overall IT security programs and ensures compliance with relevant standards and guidelines.
IT Steering Committee	Sets strategic direction, policies, procedures, and guidelines for institution-wide data administrative activities; establishes security standards for administrative data, in order to promote and protect the institution's interests in it.
Director of CNS	Sets strategic direction, develops overall policies, coordinates, and provides services supporting institution-wide data administration activities.

For detailed description of the various Administrative Data Roles refer to Appendix-A.

3. Responsibilities of Administrative Data Users

Use of administrative data only in the conduct of institutional business

- The University expressly forbids the disclosure of unpublished administrative data or the distribution of such data in any medium, except as required by an employee's job responsibilities and approved in advance by the data steward. In this context, disclosure means giving the data to persons not previously authorized to have any type of access to it. The University also forbids the use of any administrative data for one's own personal gain profit, for the personal gain or profit of others, or to satisfy personal curiosity.

Maintenance of confidentiality and privacy - Users will respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to data they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information. All data users having any access to legally restricted or limited-access data will formally sign a Privileged Access statement to acknowledge their understanding of the level of access provided and their responsibility to maintain the confidentiality of data. Each data user will be responsible for the consequences of any misuse.

Protection of data - Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted the ability to view, copy, download, create, modify or delete. This includes the requirement that they maintain their personal computing environments, whether on-campus or off-campus, in accord with the University's AUBede security mandates and recommendations.

Accurate presentation of data - Users will be responsible for the accurate presentation of administrative data, and will be responsible for the consequences of any intentional misrepresentation of that data.

Maintenance of data quality - Users are responsible for notifying data stewards or data security contacts when they recognize that data is in error, incomplete, obsolete or missing.

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.

Appendix-A

Detailed Description of Administrative Data Roles

System sponsors/Data stewards (used interchangeably) are senior institutional officials, Vice President or department head with policy-level responsibility and accountability for data, including creation and maintenance, within their appropriate data domains. They ensure the usability, reliability, availability and integrity of information systems and their data by serving as liaisons between each system's stakeholders. They negotiate priorities and enhancements to the systems and lead change management processes in accord with the documented strategic goals for particular systems. They are responsible for ensuring that the system for which they serve as sponsor is operable and available to all authorized users on an established schedule. They also serve as liaisons between the stakeholders and the technical staff responsible for such systems and the infrastructure in which they operate. They notify technical staff and stakeholders of required changes. They provide resources and training to those with other data-related roles to assure that quality standards are met. As data stewards, their specific responsibilities include:

- Assigning each item of administrative data to a data category.
- Defining the criteria for archiving the data to satisfy mandated and business-driven retention requirements, with advice from legal counsel, business process owners, database administrators and backup administrators on the balance of cost effectiveness and reasonableness.
- Determining the business needs for security for their data and monitoring and reviewing security implementation and authorized access, in consultation with the CNS Security officer.
- Establishing procedures for initial definition and change of data elements within their data domains.
- Providing data descriptions for directories that will let data users know what shareable data are available, what the data mean, and how to access the data stored within the repositories for which they are responsible. Data definitions will be: based on actual usage, made according to University standards, modified only through approved procedures, and reviewed on a timely basis and kept current.
- Developing policy to promote the accurate interpretation, responsible use and protection of administrative data in their domains.
- Specifying data viewing, copying or downloading procedures that are unique to a specific data repository or set of data elements. These procedures will ease "read-only" access, will preserve data quality and will minimize security risk.
- Ensuring the rules and conditions that could affect the accurate presentation of data are well known by data users and processors and supporting users/processors in the use and interpretation of administrative data, primarily through documentation, training, and problem resolution.
- Ensuring data quality by:
 - Determining the most reliable sources of data and regularly evaluating the quality of the data.

- Assigning and overseeing data entry, data capture and maintenance to ensure data quality.
- Identifying gaps and redundancies in the data and, to the extent possible, ensuring that only needed versions of each data element exist.
- Specifying data control and protection requirements to be observed by data processors and users.
- Informing the system sponsor of any new data needs, gaps in quality, and/or removal of data redundancies or obsolete data.
- Generally monitoring the data for accuracy, integrity, and dependability, and where appropriate, initiating action concerning these issues.

Data security contacts carry out the data domain policies set by the data stewards, as well as the institution's overall administrative data security policies. Data security contacts are responsible for making known the rules and procedures to safeguard the data from unauthorized access and abuse. They also play an active and critical role in data access authorization processes. Access in this context means either (a) the capacity for data processors to enter, modify or delete data or (b) the capacity for data users to view, copy or download data. The access-authorization responsibilities of data security contacts include:

- Approving access requests for employees and sponsored individuals by their departments' heads and forwarding these to the next stop in the approval chain
- Requesting adjustments to these authorizations when access needs of employees and sponsored individuals within their departments change.
- Regularly verifying the accuracy of existing authorizations for individuals in their departments and monitoring for inappropriate access activity.

Data security contacts who report to a data steward are typically also assigned responsibility for approving all or selected requests from other departments to access data in that data steward's data domain. In some cases, data stewards have granted blanket access for selected data on condition that the requestor satisfies certain prerequisites (e.g., signing a confidentiality agreement)

Data users are, in this context, any institutional employees who use institutional administrative data -- persons who view, copy or download data, but who do not enter, modify or delete it. Persons who view data and who copy or download it are responsible for the accurate presentation of that data. They also are responsible for helping to protect the data to minimize security risks and for helping to monitor data quality.

Data processors are persons specifically authorized by data stewards to enter, modify, or delete data. They are responsible for and accountable for completeness, accuracy, and timeliness of the data, and they are cognizant that other persons rely on their products for those qualities.

CNS - Application Specialists/Database administrators (used interchangeably) develop, communicate and monitor compliance with standards for the management of institutional data and for ensuring that data are accessible to those who need it. They work closely with the system sponsors/data stewards on formulation of data policies, standards, and procedures. They also work with the system sponsors/data stewards to establish long-term direction for effectively using information resources to support institutional goals and objectives. The database administrators develop the overall data architecture and create logical data models for data repositories. These models are ultimately used to create an institution-wide data model that cross-references data across applications and encourages data sharing. The data administrators develop standard methods for naming and defining data. They also facilitate conflict resolution in data definitions. They provide means that enable institutional data to be available to authorized users in a manner consistent with established data access rules and decisions. The data administrators develop, communicate and promote standards for data quality, as well as model-processes for assuring it. In conjunction with the security officer, they develop and promote processes to minimize security risks.

CNS - Security Officer work closely with data security contacts, and where appropriate Human Resources, to administer data authorization processes for enterprise-wide administrative data . They establish/delete user IDs and grant/remove access to users with proper authorization and manage password expiration and reset processes. They also distribute and monitor data security contact usage of administrative data security reports and investigate unauthorized access in collaboration with the internal auditor.