DALHOUSIE UNIVERSITY
Inspiring Minds

Policy

Data Administration

Policy

Area:	**Date Issued:** April, 1994
Title: Data Administration	**Last Revision Date:** January 9, 2004
Issued by: Vice President, Finance & Administration	**Approved by:** President

A. INTRODUCTION

The President established the Committee on Data Administration (CODA) in May, 1992, to advise him on policies in the area of data administration (attached as references Policy ADC 011 and TOR for CODA). As an initial task, CODA reviewed data administration guidelines that have been adopted at other universities and, adjusting for differences in Dalhousie's environment, developed a draft set of guidelines for discussion purposes.

These guidelines were presented to the University community at a well-attended meeting in November 1992 and were subsequently discussed in small group interviews with a wide array of interested and affected parties. The interviews provided some very thoughtful suggestions for improvements to the draft guidelines. The guidelines, amended as a result of the input received, were presented for Presidential approval in November 1993 in the form of a document entitled "Report of the Committee For Data Administration on the Development of Data Administration Guidelines."

The Report was approved by the President in April, 1994 and from that date operated as the governing data administration policy. In the intervening years an integrated suite of administrative applications was developed. The Banner Implementation Integration Policy Advisory Committee (IPAC) was established in May, 1998 to advise and resolve business issues arising from the implementation of those administrative applications and to assume the role of CODA.

At the request of the President, in the Fall of 2003 the guidelines were reviewed and minor changes were made and reflected in this document.

In November, 1993, CODA described the nature of its undertaking in the following way:

> One of the objectives of the University's approved long-range plan for Administrative Computing is the development of distributed administrative computing processes. The evolution to a decentralized data environment requires that an organization come to grips with some critical issues, including those involving data access, integrity, manipulation and reporting. Perhaps the most important and politically sensitive is that of data access. This issue is further compounded by legitimate concerns regarding legal requirements, data security, and data validity.
>
> A data custodian can be reluctant to provide open access to data for fear the data will be

> misunderstood and misused. Data with implications for funding allocations, program evaluation or salary relationships can be viewed as extremely sensitive. Users of information need to demonstrate responsibility and understanding of the intricacies and anomalies of data.
>
> On the other hand, custodians can view expanded access as an opportunity to provide an increased level of data quality and/or achieve increased operational efficiency. Users who see a direct link between the quality of data entered into a database and the quality of data and reports they can access will be more conscientious in reporting and auditing data. Expanded data access can address concerns that inequities exist, in resource allocation or academic workloads for example.
>
> In the end, however, the degree of data access that is provided in a university becomes essentially a question of policy and leadership philosophy.

These statements are equally applicable ten years later. The underlying policy of ensuring access to data where required within the university while safeguarding privacy remains the same.

B. DEFINITION OF TERMS

1) **Institutional Database**: A subset of the university's data made up of those data elements that are relevant to institutional management can be thought of as forming a single, logical database, referred to as the Institutional Database (IDB). Elements of the IDB may reside in different database management systems, or on different machines and may be collected, used and maintained by either academic or administration units.

2) **Data Element:** A data element is considered to be part of the IDB if it satisfies one or more of the following criteria:

a) It is relevant to planning, managing, operating or auditing a major administrative function of the university.

b) It is referenced or required for use by more than one organizational unit.

c) It is included in an official university administrative report.

d) It is used to derive an element that meets one or more of the criteria above.

3) **Data Custodian:** A data custodian is a university official who has planning and policy-level responsibilities for data in his/her functional area (e.g. the Registrar, the Director of Financial Services). Every element of the IDB is the responsibility of a uniquely designated data custodian, with the exception of the Student Information System, which operates by a committee chaired by the Vice-President Student Services. Data custodians may identify and/or assign data stewards and may delegate responsibility to them.

4) **General Custodian:** A data custodian who has planning and policy level responsibilities for cross-module or "general" areas that intersect functional areas is termed a General Custodian. Use of the term "Data Custodian" throughout this policy shall include the term "General Custodian" with necessary changes in point of detail.

5) **Data Steward:** University officials and staff who have operational responsibility for information management activities related to the collection, maintenance and dissemination of institutional data are termed data stewards (e.g. the Associate Registrar, Student Information; the Manager of Systems and Information Management, Financial Services). Data stewards may delegate responsibility to systems security officers.

6) **Systems Security Officer:** University staff who have operational responsibility to implement administrative system access are termed systems security officers.

7) **Data User:** Data users are University officials and staff who have operational responsibilities to use institutional data to perform their specifically assigned job function.

8) **Data Administration:** Data administration is the function of applying formal guidelines to the management of the University's data system.

9) **Data View:** A data view is a logical collection of data elements, possibly from multiple physical databases, which are assembled and presented according to a defined set of rules.

10) **Data Model:** The institutional data model is a description of all major data entities in the IDB and the relationships among these data entities.

11) **Data Architecture:** The design and structure of an enterprise's data, data relationships, and data system.

12) **IPAC:** IPAC is a committee established in May, 1998 among whose responsibilities include recommending overall policy and guidelines for management of and access to the institutional data of the University. IPAC also regularly reviews the performance of the overall data administration function.

SCOPE OF POLICY

All data regarding the operations of the university that are recorded using university resources are the property of the university. These data will vary in their relevance to the institutional administrative processes. Nevertheless, data administrative policies should be applied as uniformly as possible to all elements of the IDB as part of a coordinated data administration effort.

FEATURES OF THE INSTITUTIONAL DATABASE

1) **Data Collection and Maintenance:** The data custodian is ultimately responsible for complete, accurate, valid and timely data collection, and for ensuring that the data collection is related to a university purpose. Data stewards may be delegated responsibility for data collection and maintenance under the authority of the data custodian.

2) **Data Security and Storage:** Administrative Computing Services will provide a technical architecture for data storage and security which supports the guidelines and policies set out by IPAC. The data custodian in concert with Administrative Computing Services will determine appropriate policies and procedures to ensure that data are backed up, that archival requirements for storing and preserving historical data encompass all defined data elements, and that appropriate authentication procedures are in place. Data custodians in concert with data stewards as supported by systems security officers will be responsible for administering systems access, for identifying potential security breaches and addressing actual security breaches.

3) **Data Meaning and Documentation:** The data custodian is ultimately responsible for the meaning and documentation of data elements. The data custodian will ensure consistency and continuity of the meaning of data elements, whenever changes or additions are proposed to data

elements for which (s)he is responsible. Documentation for each data element should include information pertaining to its unique description, frequency of use and location, and other attributes.

Administrative Computing Services is responsible for maintaining a single, universal data dictionary for documenting institutional data elements. Administrative Computing Services will also be responsible for the data administration function of creating and maintaining the University's institutional data model, which will be supported by the universal data dictionary.

The attributes for inclusion in the documentation process should be determined by the custodian and Administrative Computing Services.

4) **Data Integrity, Validation and Correction:** The data custodian or steward who has been assigned the delegated responsibility must ensure data integrity, respond to questions relating to data accuracy and correct inconsistencies as necessary. Edit and validation checks will be incorporated into any IDB data applications to assure the accuracy and integrity of the data. Where incorrect data are identified, the data custodian must identify the cause and make the necessary adjustment and notify all data users who have received or who have had access to the incorrect data.

5) **Data Access:** Consistent with the intent of the distributed policy for managing aspects of Administrative Computing, access to institutional data must be promoted to ensure an effective data administration policy. Data custodians must designate each data element that is restricted and define the extent and nature of the restriction. Access to unrestricted data will also be available to other members of the university community, such as student senators and members of the Board of Governors. (see Section E.)

It is important to distinguish between RECORDS (which are specific aggregates of data elements attached to an identifying person, unit, or occurrence), and the unidentifiable DATA represented by a collection of records. Access to data refers primarily (though not exclusively) to the latter. Access to identifying characteristics either in the records, or implicitly in certain profiles of data, may be restricted as indicated below.

Further manipulations or derivations from data provided pursuant to this policy shall be clearly labeled "unofficial."

Restricted data would include those data for which data users must obtain individual authorization prior to access or to which only limited access may be granted. In determining the designation of data as restricted, reference must be made to the legal, ethical or other constraints which require this restriction. The restriction must describe the data users who are typically given access to the data, under what conditions or what limitations.

A data view will not necessarily inherit the restriction characteristics of individual data elements since the removal of, for example, personally identifying data elements, could result in a view that is not restricted.

Each data custodian will be individually responsible for documenting data access procedures that are unique to a specific information resource or set of data elements, and will work with Administrative Computing Services in ensuring that a single set of procedures for requesting permission to access restricted data elements is established.

All requests for access to institutional data are to be directed through the appropriate data steward.

Under certain circumstances a data user may request that IPAC review the restrictions placed on a data element or view or review a decision to deny access to restricted data. (see G6.)

6) **Data Availability and Integration:** Data custodians are responsible for making institutional data available to data users within a reasonable timeframe. Administrative Computing Services working with data custodians will be responsible to ensure data compatibility, accessibility and the development of appropriate interfaces among institutional data elements.

7) **Data Destruction.** Data custodians are responsible for implementing policies and procedures established by IPAC concerning the destruction of data when it is no longer reasonably required for university purposes.

ROLE OF THE USER

Individuals who are given access to university data must accept the following responsibilities:

1) The granting of access to university data is done based on an individual's specifically assigned job function. An individual's designated role within the Board of Governors or Senate and the respective committees would also be considered reason to grant access to university data (reference Section D, Article 5). Any use of university data for purposes other than for the undertaking of assigned responsibilities or roles is prohibited.

2) Individual data users who identify possible improvements in a component of the institutional database either through system changes or through the development of new data views are asked to submit a request for changes for review and approval to the data custodian responsible for that component of the institutional database.

3) Users are responsible for ensuring they use university data in a fashion consistent with the definition of the data, and for the purposes for which the data has been collected. Data users should contact the appropriate data custodian or steward if they have any questions regarding data definitions and/or data uses. Any further manipulations or derivations of university data shall be clearly labeled "unofficial."

ASSOCIATED ROLES OF THE DATA CUSTODIAN AND ADMINISTRATIVE COMPUTING SERVICES

To ensure the effective use of the institutional database and the development of distributed administrative computing processes, user support and system administration functions will need to be provided.

1) **User Support:** Subject to the availability of financial resources, data custodians will provide user support, primarily through documentation of the information resource, but also as needed in the form of an advisory service and training sessions, to assist data users in the interpretation and use of data elements in the IDB for which they have responsibility. Enquiries concerning modifications to the system must be directed to the custodian responsible for that component of the institutional data base. These activities may be delegated to data stewards.

2) **System Administration:** Administrative Computing Services (ACS) will be responsible for developing the overall data architecture for the university, maintaining a central data dictionary for data custodians, and for assisting application systems developers and data users in the use of the data dictionary.

ACS will also be responsible for providing appropriate system software and hardware for data storage, access, security and control, and for providing technical training and consulting support to users of data.

ACS will ensure that new systems development or modifications to existing systems comply with data administration objectives including compliance with recommended technical platforms and other standards, as established by ACS from time to time.

ACS will modify its system development methodology so as to properly express the new relationships and responsibilities among clients, system developers, and the data administration function.

ROLE OF IPAC

IPAC has the authority and responsibility to:

1) Recommend new policies, and changes in established policies, that are relevant to the management of the institutional database;

2) Identify the official data source when overlaps occur in various systems;

3) Authorize tests, audits, validation checks, controls and check-points in terms of amending update or data creation procedures. If new University data is to be created by a procedure, or if existing procedures are to be altered substantially, IPAC must reaffirm those attributes which it administers, vis à vis custodianship, stewardship, security updating control, etc;

4) Create task groups to ensure consistent definition of data elements throughout the University; and

5) Review particular applications of the data administration policy, at the request of a data custodian or data users, but only if appeals through the normal management structure have been exhausted. In such circumstances, IPAC will attempt to obtain a mutually agreeable resolution of the difficulty, and, failing such resolution, will recommend appropriate remedies to the President.

Revision History

April, 1994	version 1.0
January 9, 2004	revision