

The University of the District of Columbia

INSTITUTIONAL RESEARCH



ASSESSMENT & PLANNING

Data Management Policy

OFFICE OF INSTITUTIONAL RESEARCH, ASSESSMENT & PLANNING
4200 Connecticut Ave. NW
Bldg 52 Fifth Floor
Washington, DC 20008
(202) 274-5012 FAX (202) 274-6921
www.udc.edu/irap

THE UNIVERSITY OF THE DISTRICT OF COLUMBIA

Office of Institutional Research, Assessment & Planning



Data Management Policy

David D. Caruth, Ph.D., Director
Diane Hayes, M.A., Operations Research Analyst
Gashaw Mekonnen, M.S., Senior Operations Research Analyst
Marie Racine, Ph.D., Professor/Assessment Coordinator
Latresa Stewart, B.S., Office Manager

University of the District of Columbia
Office of Institutional Research, Assessment and Planning
4200 Connecticut Avenue, N.W.
Building 52, Suite 506-F
Washington, DC 20008
Telephone: (202) 274-5012
Facsimile: (202) 274-6921



January 19, 2007

Dear Colleagues and Friends of UDC:

In October, 2006, the Executive Cabinet of the University of the District of Columbia approved the formation of the Institutional Research Data Management Committee (IRDMC). Under the leadership of the Director of the Institutional Research Assessment and Planning office, the IRDMC was charged with developing Data Management Policy guidelines for the University; identifying appropriate data user classifications according to various levels of security for internal and external requests for data; and identifying appropriate data user classifications according to various levels of security for internal and external use of institutional data.

It was agreed that each Vice President, the CFO and CIO shall appoint one member to serve on the IRDMC. However, because of the size and complexity of both Student Affairs and Academic Affairs, those VP's would be allowed to appoint 2 members with one member from Athletics and one appointment coming from the COES division. The Provost/Vice President for Academic Affairs (or her/his designate) shall serve as an ex-officio member.

Following several meetings, including input from the Executive Cabinet, and the leadership of the academic community, I am pleased to submit the University of the District of Columbia's Data Management Policy guidelines. Our aim is to streamline the flow of data from our office to those of you who rely upon gaining access to institutional data for decision making and planning purposes.

Sincerely,

David D. Caruth

David D. Caruth, Ph.D.
Director

TABLE OF CONTENTS

	Page
I. PURPOSE.....	1
II. INTRODUCTION.....	1
III. DEFINITIONS.....	2
IV. POLICY.....	3
A. Ownership.....	3
B. Data Management.....	3
1) IR Data Management Committee (IRDMC)	3
C. Data Classification and Access.....	4
D. Roles and Responsibilities.....	5
1) Data Stewards.....	6
2) Data Managers.....	6
3) Supervisory Personnel.....	7
4) Data User Responsibilities.....	7
E. University Data Request.....	8
F. IR Data Security.....	8
V. REFERENCES.....	8

University of the District of Columbia Office of Institutional Research, Assessment and Planning Data Management Policy

I. PURPOSE

Institutional Data is a valuable University asset. Data is information about University constituencies, students, faculty and staff, resources (funds, space, etc.) that is collected and used in the day-to-day operations of the University. It is used as the basis for administrative reports, both internal and external to the University. Data enables administrators to assess the needs of the University community and modify services accordingly. It is vital not only in the day-to-day operations of the University, but to short and long-term planning as well.

The purpose of this policy is to protect, maintain and centralize this valuable asset, permit the sharing of Institutional Data through accurate and consistent definitions, and provide a coordinated approach to its use and management. In all cases, applicable District and Federal statutes and regulations that guarantee either protection or accessibility of institutional records take precedence over this policy.

II. INTRODUCTION

Institutional Data is an essential part of the University's information resources. Information resources include any information in electronic or audio-visual format, or any hardware or software that makes possible the storage and use of such information. This definition includes, but is not limited to electronic mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, and electronic communication systems. The use and management of University Data shall be governed by this policy.

Institutional Data consists of data that is acquired or maintained by University employees in performance of official administrative job duties. Typically, this is data that is: relevant to planning, decision making, managing, operating, or auditing major functions at the University; referenced or required for use by more than one organizational unit; or, included in an official University administrative report. Examples of system/databases that contain Institutional Data include, but are not limited to:

- Academic Records Systems (ARS)
- Alumni

- Benefits
- Billing and Receivable Systems (BRS)
- Board of Trustees (BOT)
- Budget
- Development
- Financial Accounting System (FAS)
- Financial Aid Management Systems (FAMS)
- High School Services Faculty
- Human Resource Systems (HRS)
- Job Application
- Office of Sponsored Projects
- Parking Permits
- Property Management
- Scheduling
- Space

Specifically excluded from the definition of Institutional Data are:

- Personal medical, psychiatric, or psychological data for both employees and patients seen at University Clinics;
- Notes and records that are the personal property of individuals in the University community;
- Research notes, data and materials;
- Instructional notes and materials;
- And most data that results from sponsored research projects.

III. DEFINITIONS

- A. Access – the right to read, copy, or query data.
- B. Data – the electronic or paper representation of discrete facts.
- C. IR Data Administration – the function of applying formal guidelines and tools to manage the University’s data resources.
- D. Data Dictionary – a repository that contains comprehensive information about Institutional Data.
- E. Data Managers – University officials and their staff who have operational-level responsibility for data capture, data maintenance, and data dissemination.
- F. Data Stewards – University officials who have policy level responsibility for managing a segment of the University’s data information resource.
- G. Data Users – full-time and appropriately designated part-time employees of the University of the District of Columbia who access Institutional Data in performance of their assigned duties.
- H. Institutional Data – data that is acquired or maintained by University employees in performance of official administrative job duties.

Specifically excluded from the definition of Institutional Data are: personal medical, psychiatric, or psychological data for both employees and patients seen at University Clinics; notes and records that are the personal property of individuals in the University community; research notes, data and materials; instructional notes and materials; and data that results from sponsored research projects.

- I. Institutional Research, Assessment and Planning Data Management Committee (IRDMC) – the committee that establishes policy guidelines for the management of and access to the University’s Institutional Data.
- J. Institutional Data Model – a diagram that illustrates the data entities that comprise the Institutional Database and the relationships among those entities.
- K. Institutional Database – the physical implementation of the Institutional Data Model. The database is a combination of (1) centrally stored data elements, and (2) non-centrally stored data elements.
- L. Shared data – a subset of Institutional Data that is updated by more than one organizational unit.

IV. POLICIES

A. Ownership

The University as a whole owns all Institutional Data and the subsets thereof. Various units within the University (e.g. Athletics, Financial Aid, Registrar, Human Resources etc.) generate operational data and report to their respective oversight agencies. Generally, they are the primary custodians of their own data. The administration and operational control of selected Institutional Data resides with the Office of Institutional Research, Assessment and Planning.

B. Data Management

Institutional Data will be compiled, analyzed and managed by the IR Office according to office policy and IR Data Management Policy. IR Office Policy governs the internal functions of the IR office and is separate from IR Data Management Policy.

IR Data Management Committee (IRDMC)

The IR Director (or his/her designate) will Chair the IRDMC. The (IRDMC) was created to recommend policy guidelines for the management of and access to the University’s Institutional Data.

At the discretion of the IRDMC Chair, the IRDMC may form subcommittees and task forces as needed to manage, access, store and maintain Institutional Data.

IRDMC members are appointed by the IR Director and University Vice Presidents. The IR Director shall appoint members as needed while each Vice President, the CFO and CIO shall appoint one member to serve on the committee. However, because of the size and complexity of Academic Affairs and Student Affairs, those VP's may appoint 2 members to the committee with one member from Academic Affairs coming from the COES division and one member from Student Affairs coming from Athletics. The Provost/Vice President for Academic Affairs shall serve as an ex-officio member. VP appointments may include Supervisory Personnel, Data Stewards, Data Managers, Data Users, University computing services, and other campus employees.

It is the responsibility of the IRDMC to develop procedures for IRDMC appointment term lengths; establish dispute resolution processes, and to recommend possible solutions to the appropriate Vice President. Other IRDMC responsibilities include:

- a. Data Definitions – creating standard definitions for shared data elements.
- b. Develop Procedures for Standardizing Code – determine code values and coordinating maintenance of look-up tables used for Institutional Data.
- c. Determining up-to-date Precedence – when multiple sources for data exist.
- d. Data Reliability – determining the most reliable source for data.
- e. Identifying Data – Identifying data entities and data sources that comprise Institutional Data. As this is an on-going process, the Committee will add data entities and sources to the IR Database as circumstances require.
- f. Other Duties as Assigned.

C. Data Classification and Access

All Institutional Data will be classified as being Public, University-internal, or Limited-access. The permission to access Institutional Data will be granted to all eligible employees of the University for legitimate University purposes according to the data classification under the direction of the IR office or other authorized personnel.

If Institutional Data is requested by an off-campus entity or by a University employee or representative for non-University purposes, the IR Office will identify the appropriate classification for each data element according to IR Data Management Policy and will determine the conditions under-which data will be released. Individual units will adhere to these guidelines if they receive external requests for Institutional Data under their control.

Institutional Data requested from, by or about the UDC Board of Trustees, shall be generated and/or approved by the IR Office. The IR Office will administer data requests, collect institutional data, and identify the appropriate classification for each data element according to IR Data Management Policy. Prior to its release, Institutional Data will be submitted to the appropriate VP for review. Upon review, the IR Office will forward data to the UDC Office of the President who shall have the responsibility of releasing selected Institutional Data to the UDC Board of Trustees.

For University data users, Institutional Data is classified by the IR Data Management Committee according to the following levels of required security.

1. Public Data – is available to the general public; no prior authorization is required.
2. University-internal use Data – is available to all eligible employees without restriction for use in conducting University business.
3. Limited-access Data – will be made available to eligible employees who need access to such data to perform their job duties and have received authorization from a Data Steward under the guidelines established by the IR office.

D. Roles and Responsibilities

It is the responsibility of each academic and administrative unit and/or division within the University to prepare data under its control for electronic delivery to the IR office upon request. The IR office will collect, analyze and report the findings of selected Institutional Data to stake holders. The IR office is not responsible for providing scanning services to any University office or division. It is important to note that one individual in an office may perform any combination of the functions of the Data Stewards, Data Managers and/or Supervisory personnel. The roles and responsibilities of Data Stewards, Data Managers, Supervisory Personnel, and Data Users are defined in part as follows:

1. Data Stewards

Data Stewards are individuals who have administrative and management responsibilities for segments of Institutional Data within their functional areas. Specific responsibilities include:

- a. Access – processing requests for access to Limited-access data.
- b. Data Classification – classifying each data element according to University definitions (Public, University-internal, Limited access).
- c. Documentation – ensuring that proper documentation exists for each data element.
- d. Data Quality – ensuring integrity, correction and accuracy of data and implementing programs for data quality improvement.
- e. Data Storage – identifying official storage locations and determining archiving requirements for data elements.
- f. Other Responsibilities – as set forth by IR policy.

2. Data Managers

Data Managers coordinate Institutional Data management tasks with Data Stewards, other Data Managers, and IR personnel. Specific responsibilities include:

- a. Access – defining and documenting data access procedures that are unique to a specific information resource or data set elements.
- b. Data Collection and Maintenance – ultimately responsible for collecting complete, accurate, valid and timely data, and maintaining data.
- c. Data Security – monitoring access and defining data recovery procedures.
- d. Documentation – ensuring adequate documentation exists for each data element under their purview.
- e. Other Responsibilities – as set forth by IR policy.

3. Supervisory Personnel

Every University employee who has supervisory responsibilities and is involved with the maintenance of or use of Institutional Data is responsible for implementing and ensuring compliance with IRDMC policy and for initiating corrective action if needed. In implementation of this policy, each supervisor is responsible for:

- a. Communicating IRDMC policy to employees.
- b. Establishing specific goals, objectives, and action plans to implement the policy and monitor progress in its implementation.
- c. In coordination with appropriate Data Stewards, developing plans for information systems and database development that satisfy both departmental and institutional data collection needs.
- d. Actively supporting strong data management through the IR office and unit Data Stewards.
- e. Providing education and training in data management to employees.

4. Data User Responsibilities

All data users are expected to:

- a. Access Institutional Data only in their conduct of University business.
- b. Review information created from the data to ensure, to the extent of their ability, that the analysis results are accurate and the data has been interpreted correctly.
- c. Respect the confidentiality and privacy of individuals whose records they have access to.
- d. Observe any ethical restrictions that apply to data to which they have access.
- e. Abide by applicable laws or policies with respect to access, use or disclosure of information.
- f. Provide feedback on the application of the Institutional Research Data Management policy to the IR Director.
- g. Actions contrary to these expectations are considered misuses of University property.

E. University Data Requests

The initial point of contact for access to, or use of, Institutional Data is either the Office of Institutional Research, Assessment and Planning or other authorized personnel.

F. IR Data Security

Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with IR policies and practices. The University reserves the right to use all available legal means to protect institutional data as a valuable asset.

V. REFERENCES

The Institutional Research Data Management Committee was created by the Executive Cabinet on October 24, 2006.