UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Administrative Data Management	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A015-018-01
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 March 1, 2017

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the requirements that follow have been identified to promote the best balance possible between information security and academic freedom.

I. PURPOSE:

Administrative data have value to the University and should be considered and managed as a basic resource. This policy identifies responsibilities University organizational units have with respect to the creation, maintenance and control of administrative data.

The long-term goal is the organization and control of the University's data for the purpose of making those data available as requirements dictate. Included are the inventory (identification of specific data to be managed), documentation, control and protection.

II. SCOPE:

[Intentionally omitted.]

III. POLICY:

Administrative data are basic organizational resources which should be properly managed consistent with the intent of the Federal Privacy Act.

- Data residence is determined by the degree of data sharing. Data widely shared throughout the University will reside in a central facility accessible to those who are authorized and require access. Data shared by a relatively small subset of the University community may reside non-centrally.

- The level of control and protection will depend upon the nature of the data and the extent needed for conducting University affairs. The Vice President for Information Technology has the overall responsibility for data control and centralized data registration. Individual organizational units are responsible for the creation and maintenance of particular data types, content, accuracy, and authorization of access rights to other organizational units.

- Physical integrity (protection from hardware and software failure) and organization of data stored electronically are the responsibility of the organizational unit managing the computer facility in which the data reside.
- Conflicts which may arise between organizational units such as those relating to data definition, residence, access rights, or control will be resolved by the Vice President for Information Technology and may be appealed to the Information Technology Advisory Committee.

Conflicts which may arise between organizational units such as those relating to data definition, residence, access rights or control will be resolved by the Vice President of Technology and may be appealed to the Information Technology Advisory Committee.

IV. DEFINITIONS:

University – “University” refers to the University of Miami as a whole and includes all units.

V. PROCEDURE:

While the long term goal is to manage all data of material value, the exigencies of the University’s situation dictate that implementation efforts be prioritized. The priorities are:

- Data created and accessed by new administrative systems implemented on the central computer facility.
- Other data stored electronically at the central facility
- Data stored manually

Sanctions:

Accounts and network access may be administratively suspended with or without notice by the University when, in the University judgement, continue use of the University’s resources may interfere with the work of others, places the University or others at risk, or violates University policy.

Knowing violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and /or suspected violations must be reported to the applicable System Administrator, who will report, as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.

Penalties may include:

- Suspension or termination of access to computer and/or network resources;
- Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
- Suspension or termination of contract computer and/or network services; or
- Criminal and/or civil prosecution

Enforcement:

Chief Information Security Officer or Designee (CISO) is responsible for monitoring the enforcement of this policy.