I. **Introduction (Purpose and Intent)**

Information is an integral part of the business and academic functions of the University of South Florida System (USF System); consequently, data is an important institutional resource. In order to make appropriate decisions, Institutional Data must meet basic standards. It also must be accurate and verifiable. The value of the data maintained by the USF System increases through its widespread and consistent use, and it diminishes through misuse, misinterpretation, or unnecessary restrictions on its access.

II. **Definitions**

**Institutional Data** - Institutional data is defined as all data elements created, maintained, received, or transmitted as a result of business, educational or research activities of a USF System unit and may include one or more of the following characteristics:

- Relevant to the operations, planning, controlling, or auditing of business functions of both administrative and academic units.
- Generally referenced or required between more than one administrative and academic unit.
- Included in an officially published USF System report.
- Generated or derived by any entity of the USF System or employee, or an affiliate or agent of the USF System.
- Classified and constrained in accordance with USF System, state, and federal laws and policies.
It is not the intent of this policy to supersede individual control of data or information created through teaching and research activities of faculty members as set forth in USF System regulations and the USF-UFF Collective Bargaining Agreement.

For the purpose of this policy, Institutional Data Stewardship Committees are groups formed around specific data systems which include the owners of data stored in the system. Examples of such committees are the Student Information System Advisory Group and the PeopleSoft Directors Group.

III. Statement of Policy

Institutional Data is the Property of the USF System and is not "Owned" by Any Individual, Academic, or Business Unit - Data and the meta-data about that data are business and technical resources owned by the USF System. All employees must recognize that the proper management of strategic Institutional Data is critical to the success of the organization.

Stewardship Committee responsibilities:

• Inventory Institutional Data under their jurisdiction.
• Establish rules and standards for disclosing and authorizing access to Institutional Data.
• Assume responsibility for data under their control.
• Deploy procedures to comply with regulatory rules for disclosing, categorizing, and authorizing access to administrative data.
• Deploy procedures for meeting minimum standards for data security according to data classification.
• Stewardship Committees may choose to assign responsibility for control of the data to another individual or group of individuals under the Committee’s supervision.

Data Custodians are the individuals responsible for the execution of Stewardship Committee procedures for disclosing, categorizing, and authorizing access to administrative data. They are also responsible for executing the procedures for meeting minimum standards for data security according to data classification.
Institutional Data Must Be Modeled - All strategic Institutional Data shall be modeled, named, and defined consistently (according to standards) across the business and academic divisions of the USF System. Every effort must be made by management to share data across divisions, and not to maintain redundant data without justification. Stewardship Committees responsible for the data must recognize the informational needs of downstream processes and academic units that may require said data.

Institutional Data Must Be Maintained Close to Source - All Institutional Data shall be created and maintained as close to the source as feasible. Data quality standards shall be managed and applied actively to ensure reliability levels of Institutional Data as defined by the business and academic units.

Institutional Data Must Be Safe and Secured - Institutional data in all electronic formats shall be safeguarded and secured based on recorded and approved requirements and compliance guidelines. These requirements are to be determined by the Stewardship Committee Data in conjunction with the Office of Information Security. Additional policies and standards may apply to restricted institutional data, such as USF System Policy 0-515, Protection of Electronic Personal Information, and 0-516, Appropriate Use of Social Security Numbers. Appropriate backup and disaster recovery measures shall be administered and deployed for all Institutional Data.

Institutional Data Must Be Accessible - Institutional Data and information about that data (meta-data) shall be readily accessible to all, except where determined to be restricted. When restrictions are made, the appropriate Stewardship Committee is accountable for defining specific individuals and levels of access privileges that are to be enabled. The Office of Information Security will be responsible for ensuring the proper implementation of the security controls.

*Current Responsible Office: Information Technology

*Refer to the appropriate Responsible Office website for a current name of the Vice President or other Responsible Officer.