Custodians to implement best practices. Data Stewards are the first escalation point for problem resolution.

3. *Data User*: Data Users are individuals who access institutional data to perform their assigned duties. Data Users are responsible for safeguarding their access privileges, for the use of the institutional data in conformity with all applicable University policies, and for securing such data.

4. *Data Custodian*: Data Custodians are information technology experts assigned to each transactional and reporting system which maintains institutional data. Data Custodians oversee the safe transport and storage of data, establish and maintain the underlying infrastructure, set security measures, and perform activities required to keep the data intact and available to users.

In addition, Data Custodians are responsible for working with Data Stewards to develop automated processes which identify erroneous, inconsistent, or missing data. Data Custodians work with data support groups, the Office of Institutional Research & Analysis, and Data Stewards to resolve data issues.

D. ACCESS AND CONFIDENTIALITY

1. Access to University institutional data is based on the business needs of the applicable unit.

2. Data Users will be granted secure access to view or query institutional data on a need to know basis for the purposes of performing legitimate administrative, research, academic and other official responsibilities pertaining to the mission of the University. Examples include, but are not limited to, planning, decision making, and official reporting.

a. The "need to know" basis exists when certain conditions are met, including, but not limited to:

i. The institutional data is needed to improve services to faculty, staff, students, and other University constituents.

ii. Access to institutional data increases the understanding, usefulness, and ease of use of the data, and/or maximizes efficiency of human, physical, and digital resources.

iii. Integration of institutional data with other data and information or applications increases the value of the institutional data to those who may use it.

b. Curiosity does not constitute a "need to know." Access to institutional data for academic research and inquiry may be approved subject to privacy rules and regulations, and appropriate institutional review.

c. Access to institutional data will be granted subject to best practices for data and information management and analysis and should minimize duplication of data and information capture, storage, maintenance, and retrieval.

3. In order that the proper controls are applied, it is the responsibility of each person accessing institutional data to:

a. Know the classification of the system being used.

b. Know the type of institutional data being used.

c. Follow the appropriate security measures.

d. Consult the related policies for further information.

E. TRAINING

The Data Trustees are responsible for establishing required training for individuals that manage Institutional Data, as appropriate to their role.

F. INTEGRITY, VALIDATION, AND CORRECTION

1. Institutional data must be safeguarded and managed in all formats and media (e.g., print and digital), at all points of access, and across all University systems through coordinated efforts and shared responsibilities.

2. Each Data Trustee, in conjunction with the appropriate Data Steward, shall be responsible for developing a plan for their functional area to assess the risk of erroneous or inconsistent data and indicate how such institutional data, if found, will

I. [illegible]ANCE

Failure to comply with this Policy ma