

<b>Information Resource Security Standard Administrative Procedures</b> 29.01.99.K1.260	06/14/2011 - Effective
<b>Institutional Data Management Standard Administrative Procedure</b>	07/17/2012 - Revised iTech - Author

## **Institutional Data Management Procedure**

### **Purpose**

The purpose of this procedure is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of Texas A&M University-Kingsville (TAMUK) information.

### **Audience**

This procedure applies to individuals with access to any TAMUK Information Resource.

### **Definitions**

1. **Institutional Data:** A data element qualifies as Institutional Data if it is:
  - a. Generated or collected in the course of or in furtherance of the business of the University;
  - b. Exists in digital form, capable of being electronically stored or transmitted; and
  - c. Resides or resided at any time in the past on any University-owned computer, server, or storage medium.
  - d. Paper records that do not meet these criteria are not subject to this policy, although they may be subject to other, similar policies of the University.
2. **University Data:** An Institutional Data element qualifies as University Data if it is:
  - a. Neither Unit-Specific nor Individual-Specific Data as defined below; and is
  - b. Relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or academic unit of the University; or
  - c. Generally referenced or required for use by more than one organizational unit; or
  - d. Included in an official University administrative report; or
  - e. Used to derive an element that meets one or more of the criteria above.
3. **Unit-Specific Data:** An Institutional Data element qualifies as Unit-Specific Data if it is: Uniquely pertinent to the work of a single office or unit and used and accessible solely by individuals within that office or unit. While correspondence and other documents (whether in print, electronic or digital formats) may contain University Data subject to this procedure, correspondence and documents themselves will generally not qualify as University Data applying the above criteria. Ownership of and access to correspondence and documents created or received by University personnel are governed by the Texas A&M System on Records Management, the University Intellectual Property Procedure, the Public Information Act.
4. **Individual-Specific Database:** An Institutional Data element qualifies as Individual-Specific Data if it is generated and maintained by an individual affiliated with the University as an employee, contractor, or student within the scope of that individual's relationship with the University and if it is not generally communicated to or used by other members of the University community.

### **Procedure Statement**

1. TAMUK Institutional Data, by definition, practice and intent, are University assets. Institutional Data are owned by the University and not by individual persons, units, or departments of the University.

<b>Information Resource Security Standard Administrative Procedures</b> 29.01.99.K1.260	06/14/2011 - Effective
<b>Institutional Data Management Standard Administrative Procedure</b>	07/17/2012 - Revised iTech - Author

2. Institutional Data will be safeguarded and protected. As University assets, Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction and/or inappropriate disclosure in accordance with established institutional policies and practices and federal and state laws. Data will be shared based on institutional policies. Institutional Data will be made accessible to all authorized users and systems, as defined in institutional policies.
3. Data will be managed as an institutional resource. Data organization and structure will be planned on functional and/or institutional levels. Data usage and data sources will be managed through the data stewardship principles of administering and controlling data quality and standards in support of institutional goals and objectives.
4. Institutional Data will be defined and identified. Standards will be developed for their representation in the database.
5. The quality of Institutional Data will be actively managed. Explicit criteria for data validity, availability, accessibility, interpretation, and ease of use will be established and promoted. Controls will be established to assure the completeness and validity of the data, and to manage redundancy. Action programs for data quality improvement will be implemented.
6. The Director of Planning and Assessment is responsible for the accuracy of various reports. All official reports to the State of Texas, Texas A&M System, Federal Government, and other agencies must be approved by the Director of Planning and Assessment. Reports should be submitted to this office for validation at least two weeks prior to the submission deadline. Banner and the Banner data warehouse are the official sources for student related information.

### **Procedure Requirements**

---

1. Goals
 

Successful management of Institutional Data is critical to the administrative functions of the University. Through active planning, organization, and control of these institutional assets, the University will:

  - a. Manage data as a strategic asset to improve the quality of services to faculty, staff and students.
  - b. Create data sets and implement application software that generates integrated databases that are consistent, reliable and accessible to meet institutional requirements.
  - c. Provide data management services that result in the highest quality data to all units to help maximize the efficiency and effectiveness of their processes.
2. Reason for Procedure
 

To establish procedure for the management of Institutional Data (as defined below) and the responsibilities for the protection of those data. The procedure will serve to:

<b>Information Resource Security Standard Administrative Procedures</b>	06/14/2011 - Effective
29.01.99.K1.260	07/17/2012 - Revised
<b>Institutional Data Management Standard Administrative Procedure</b>	iTech - Author

- a. Promote accuracy related to various reports from the University as required by the State of Texas, Federal Government, and other agencies.
- b. Ensure establishment, maintenance and delivery of stable, reliable, and accessible collections of Institutional Data in electronic form for shared access by the University community;
- c. Maximize the value received from Institutional Data by increasing the understanding of data and their use;
- d. Provide an integrated view of the functions of the University;
- e. Support the University's strategy to incorporate information technology as an integral part of decision-making, competitive positioning, and delivery of services.

### **Responsibilities**

Every University Dean, Department Chair, and Director is responsible for implementing and ensuring compliance with this Institutional Data Management Procedure and must initiate corrective action with the proper authorities of the University if it is needed. Responsibilities include:

1. All official university reports as defined above must be submitted to the Director of Planning and Assessment at least two weeks prior to the submission deadline.
2. Communicating this procedure to employees.
3. Establishing specific goals, objectives, and action plans to implement the data procedure.
4. Developing plans that guide information system and database development to satisfy both customers and institutional needs.
5. Actively supporting strong data management through data stewardship as defined in policies and procedures promulgated in connection with this procedure.
6. Making education and training in data management principles available to staff whose jobs require them to access maintain or use Institutional Data.

### **Disciplinary Actions**

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

### **References**

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)

<b>Information Resource Security Standard Administrative Procedures</b>	06/14/2011 - Effective
29.01.99.K1.260	07/17/2012 - Revised
<b>Institutional Data Management Standard Administrative Procedure</b>	iTech - Author

9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441