University Policies and Procedures

10-04.00 – DATA STEWARDSHIP POLICY

I. Policy Statement: Towson University ("University") expects all stewards, custodians and users of its administrative data to manage, access, and utilize this data in a manner that is consistent with the University's need for security and confidentiality. The University functional areas must develop and maintain clear and consistent procedures for access to University administrative data.

II. Reason for Policy: Maintaining the confidentiality, integrity, and availability of University data is critical to the success of the University. This policy establishes the methodology by which the University will manage its data and assigns responsibilities for the control and appropriate stewardship of University data.

III. Definitions:

1. University Data – Items of information that are collected, maintained, and utilized by the University for the purpose of carrying out institutional business even if subject to any contractual or statutory limitations. University Data may be stored either electronically or on paper and may take many forms (including but not limited to: text, graphics, images, sound, or video). Research data, scholarly work of faculty or students, and intellectual property that do not contain personally identifiable information or other data protected by law or University policy are not covered by this policy.

2. Data Steward – University official or designee having direct operational-level responsibility for information management (usually department directors). Data Stewards are responsible for data access and policy implementation issues

3. Data Custodian – Departments and/or personnel responsible for providing a secure infrastructure in support of the data including, but not limited to: providing physical security; backup and recovery processes; providing access to users as authorized by the Data Stewards; and implementing and administering appropriate levels of controls over the information.

4. Data User – Individuals who need and use University Data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and

integrity of that data. Any University employee with access to University Data can be considered a Data User.

5. University means Towson University.

IV. Responsible Executive and Office:

Responsible Executive: Vice President for Administration & Finance and Chief Financial Officer

Responsible Office: Office of Technology Services

V. Entities Affected by this Policy: All Data Stewards, custodians and users of University Data.

VI. Procedures:

A. Data Classification

All data shall be classified in one of three categories:

1. Public Data – data intended for general public use. An example is the University's online directory.

2. Protected Data – All data which are not legally restricted and which may be accessed, without restriction, by University employees in the performance of official University business.

3. Confidential Data – All data which, if released in an uncontrolled fashion, could have substantial fiscal or legal impact on the University. Examples include personal data containing elements such as Social Security Numbers, health records, credit card information, student grades, and personnel records. Personally identifiable information (other than public data [directory information as defined under FERPA, HIPAA or other federal law]) should be considered *Confidential*.

B. Roles and Responsibilities

All University employees, students, affiliates and others granted access to University Data or University information systems are responsible for understanding the terms and conditions under which they may access and use University Data. An individual may have one or more of the roles listed below.

1. Data Steward

a. Establishes definitions of the data assigned to them.

b. Develops policies, procedures and guidelines for the management, security and access to data in their control according to University policies and standards.

c. Reviews and approves users' access to data.

d. Reviews and updates user access routinely and communicates changes to Data Custodian.

e. Ensures appropriate classification of data.

f. Assists in establishing necessary security and access controls for data in electronic form.

g. Provides guidance to departments and individuals within the area of responsibility on data access and policy implementation.

h. Defines requirements for safeguarding data.

i. Ensures that security policies are implemented.

j. Delegates operational responsibilities for data.

k. Ensures that responsibilities within their office and delegated to technical administrators, third-party vendors, or other custodians are met.

2. Data Custodian

a. Provides user access to data as defined by the Data Steward.

b. Removes user access as necessary.

c. Provides a secure and stable environment for the storage of the data.

3. Data User

a. Protects all data and access to data in their care. Recipients of *Confidential Data* are responsible for maintaining the restricted nature of the data.

b. Uses data and access to data only as required in the performance of legitimate University functions and their job.

c. Adheres to applicable Federal and State laws, requirements of any applicable contracts, and University policies, standards and procedures.

C. Enforcement

Violations may result in disciplinary action in accordance with applicable University policies and procedures. Revocation or restriction of computer privileges is also possible. The Information Security Officer reserves the right to audit computer and network systems on a periodic basis to ensure compliance with this policy. Report any violation of this policy to the ISO at infosec@towson.edu.

Related Policies: TU Policy 10-01.01
TU Policy 10-01.02
TU XXX – Non-Public Information Policy

Approval Date: 04/18/2011

Effective Date: 04/18/2011

Approved by: President's Council 04/13/2011