University Policies and Procedures

10-05.00 – Data Governance Policy

I. Policy Statement: This policy applies to all individuals utilizing Towson University ("University") data at the University, including but not limited to all University faculty, staff, students, volunteers, visitors and contractors.

The University understands that data is an essential and key asset that must be managed and secured appropriately. The University has an obligation to protect the confidentiality, quality, and availability of University Data. This policy governs the confidentiality, quality, and availability of University Data and assigns responsibilities for the control and appropriate stewardship of University Data.

II. Definitions:

A. Data Governance Committee (DGC) - The DGC is the managing authority for the University's Data Governance Program. The DGC strategically and proactively addresses issues related to data and information management across the University.

B. University Data - University Data are 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.

University Data are essentially any data required to conduct the operations of the University. This includes any data elements that are created, received, maintained, or transmitted.

III. Responsible Executive and Office:
Responsible Executive: Vice President of Administration & Finance and Chief Financial Officer

Responsible Office: Office of Technology Services

IV. Entities Affected by This Policy: All divisions, colleges, departments and operating units, and University faculty, staff, students, volunteers, visitors, contractors and any other persons using University information resources.

V. Procedures:

A. Policy Principles

The purpose of Data Governance is to protect University Data and the information resources of the University from unauthorized access or damage. The underlying principles followed to achieve this objective are:

1. University Data are the property of the University and shall be managed as a key asset within Federal, State and University System of Maryland ("USM") regulations.

2. University Data shall be protected.

3. University Data shall be accessible according to defined needs and roles.

4. Data Trustees and Stewards are responsible for the subset of data in their purview.

5. University representatives will be held accountable for their roles and responsibilities.

6. Resolution of issues related to University Data shall follow consistent processes.

7. Quality standards for University Data shall be defined and monitored.

8. University metadata shall be recorded, managed, and utilized.

9. Necessary maintenance of University Data shall be defined.

10. Unnecessary duplication of University Data is discouraged.

B. Responsibilities – The DGC will follow the above principles to implement and manage this policy and will create processes and/or procedure guidelines as appropriate to ensure adherence to this policy. Individuals who are authorized access to University Data shall adhere to appropriate roles and responsibilities as defined by the DGC.

C. Maintenance – This policy will be reviewed by the University's DGC every two (2) years or as deemed appropriate based on changes in technology or regulatory requirements.

D. Enforcement – All individuals within the scope of this policy are responsible for understanding and complying with all applicable University policies, procedures, and standards for dealing with University Data and its protection. Violations of this policy may result in disciplinary action in accordance with applicable University policies and procedures. Revocation or restriction of computer privileges is also possible. The Director of Information Security reserves the right to audit the use and handling of all University Data on a periodic basis to ensure compliance with this policy. Any individual within the scope of this document that has any knowledge or suspicion of a violation or inappropriate use and/or disclosure of University Data must report it to the Director of Information Security at infosec@towson.edu. University faculty and staff should also report it to their supervisor.

Related Policies:
TU Policy 10-01.01
TU Policy 10-01.02
TU Policy 10-04.00
Human Resources Policies
USM Board of Regents Policy Section X
Code of Student Conduct
Guidelines for Responsible Computing
Data Governance Roles and Responsibilities
Standards for Data Classification

Approval Date: August 31, 2016

Effective Date: August 31, 2016

Approved by: President's Council August 10, 2016