# Towson University Confidentiality Agreement

I understand, that as a Towson University employee, I may require access to certain information to support a variety of University functions in the performance of duties as employee of Towson University. This information may include, but is not limited to, confidential or personally identifiable information about any student, employee, alumni information, and records regarding financial, business, educational, personnel, medical, and/or academic matters from a variety of media (paper and electronic) and sources including, but not limited to, interoffice communications, internal operations or publications, verbal interactions, correspondence, data, and databases (collectively, "Confidential Information").

1. **Confidentiality:** During my employment with the University, as well as after my tenure at the University, I understand that I am accountable for maintaining the confidentiality of the Confidential Information with which I work. This Confidential Information will not be revealed, copied, deleted, altered, distributed through email/file sharing, posted online, or shared with any unauthorized individual, except as required in the normal performance of my duties.
2. **Storing:** I will follow proper procedures for the storage (digital or paper) and disposal of documents and Confidential Information, as instructed and authorized.
3. **Securing**: I will take appropriate steps to secure Confidential Information. This includes, but is not limited to, safeguards such as locking my workstation, placing monitors out of the view of others, securing mobile devices and not sharing passwords. Employees are prohibited from sharing their user credentials or permitting another employee to access sensitive information in databases and/or systems.
4. **Accessing:** I will access only that Confidential Information which is required to perform duties as authorized by my supervisor. Access to Confidential Information, which includes written documents, electronic files, student educational or financial records, as well as personnel data, records or files, should be gained through normal business procedures for obtaining information. Access to Confidential Information should be limited to authorized individuals only. All employees with job duties that require accessing Confidential Information are required to safeguard such information and only use it or disclose it as expressly authorized or specifically required in the course of performing their specific job duties.
5. **Liability:** I understand that failure to abide fully with this Confidentiality Agreement is grounds for disciplinary action, up to and including dismissal from employment at the University. Additionally, I understand that disclosing data, without proper supervisor authorization, may violate the Family Educational Rights and Privacy Act of 1974 ("FERPA") and other federal and State laws and regulations that protect the confidentiality of information and records, and may subject me or the University to civil and/or criminal liability.

Visit the University's website to review Information Technology policies and standards:

- For a better understanding of how to store, secure and dispose of data properly, review the University's Data Use Standards.
- For clarification on how data is classified, review the University's Data Stewardship policy.
- For information how faculty, staff, students, volunteers, visitors and contractors utilize University data, review the University's Data Governance policy.

I agree to be bound by this Confidentiality Agreement and to take all reasonable, necessary, and appropriate steps to safeguard private data and Confidential Information from disclosure to anyone except as permitted under this Confidentiality Agreement and the policies listed above. I certify that my signature below indicates that I have read the above and understand my responsibility for maintaining the confidentiality of University information and records. I understand that, if required based on my position as an employee of Towson University and job classification, I may be required to sign a supplemental agreement.

| | |
|---|---|
| _____ | _____ |
| TU Email Address | TU Employee ID |
| _____ | _____ |
| Department | Supervisor |
| _____ | _____ |
| Signature | Date |

# Data Use Standards

## Purpose

The purpose of this document is to outline the requirements for handling and protecting all of the University's institutional data.

## Overview

Any individual who creates, processes, stores, shares, and/or destroys university data is responsible and accountable for complying with the following required safeguards for protecting data based on their classification. In addition to the following data security standards, any data covered by federal laws, state laws, regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

## Definitions

- Authentication – *Authentication* is the process of determining whether someone or something is, in fact, who or what it is declared to be.[1] For example, at Towson, individuals authenticate to most services using their NetID and password.
- Authorization – *Authorization* is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data, and application features.[2]
- Data Classification – Towson categorizes data into three types (Public, Protected, and Confidential) to provide guidance on the proper handling of that data. Definitions for each data classification can be found on the TU Data Privacy (https://www.towson.edu/dataprivacy) page.
- NetID – The *NetID* is the core computing account assigned to each faculty member, staff member, and student at Towson University. Additional information can be found on the NetID (https://www.towson.edu/netid) page.

## Required Safeguards

The safeguards that are required may differ based on the classification of the data.

Data classified as Public does not have any required safeguards defined.

**Access Control** (restricting access to data using NetIDs, permissions, or other similar methods):

- *Protected Data*:
  - Authentication (preferably, NetID-based) is required to access data
  - Authorization rules (roles, permissions, or other methods) must be defined for the data, and access to view or modify data should be restricted to only individuals who need it for business purposes
- *Confidential Data*
  - Follow all of the requirements above for Protected data
  - The individual accessing the data must have a signed confidentiality agreement on record

**Copying and Printing** (applies to both paper and electronic forms):

- *Protected Data*
    - Data should only be printed when there is a legitimate need
    - Copies must be limited to authorized individuals
    - Data should not be left unattended on a printer
    - The retention of the paper copies must follow University retention policies
- *Confidential Data*
    - Follow all of the requirements above for Protected data
    - Must have a signed confidentiality agreement on record
    - Paper/hard copies must be stored in a secure location (e.g., locked office or cabinet)

**Data Storage and Transmission** (safely storing and sending files and other data)**:**

- *Protected Data*
    - Storage on any University-managed service which uses NetID-based authentication recommended
    - Encryption is recommended for data transmission (for example, via SSL/TLS-protected HTTPS or via secure file transfer protocols such as SFTP or FTPS)
- *Confidential Data*
    - Data must be stored on the secure file-sharing service ("SecureShare"), an appropriate information system (such as PeopleSoft), or other approved encrypted storage; requests to use any other storage methods should be directed to the Office of Technology Services
    - Paper/hard copies must be stored in a secure location (e.g., locked office or cabinet)
    - Encryption is required for data transmission (for example, via SSL/TLS-protected HTTPS, via secure file transfer protocols such as SFTP or FTPS, or via the File Delivery Service email service); requests to use any other transmission methods should be directed to the Office of Technology Services

**Media Sanitization and Disposal** (safely disposing of or reusing hard drives and other storage)**:**

- *Protected and Confidential Data*
    - All electronic storage media and equipment that is owned or leased by the State (including, but not limited to: workstations, servers, laptops, cell phones, tablets and multi-function printers/copiers) must be in compliance with TU's media and equipment disposal and reuse procedures. Questions should be directed to the Office of Technology Services.

**Training and Awareness Education** (security-related training required for those handling data):

- *Protected Data*
    - General security awareness training is required
    - For system administrators, administrator-specific training is recommended
- *Confidential Data*
    - General security awareness training is required
    - For system administrators, administrator-specific training may be required
    - Applicable policy- and regulation-specific training may be required (e.g., HIPAA, FERPA, PCI)

# Questions

Questions or other comments on these standards should be direct to the Office of Technology Services (OTS). Requests for exceptions or guidance should also be directed to OTS.

Related Resources
Data Stewardship Policy;
Data Governance Policy;
Acceptable Use Policy;
Information Technology Security Policy;
**Data Privacy Web Site**

***Revision History***

| Action | Action Date | Comments |
|---|---|---|
| **Last Updated** | **11/08/2017** | |

*Source:*

1. ↑ *TechTarget*, http://searchsecurity.techtarget.com/definition/authentication
2. ↑ **techopedia, https://www.techopedia.com/definition/10237/authorization**

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

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