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**