— UNIVERSITY POLICY —

Data Classification Policy

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

The Data Classification Policy for West Chester University Information Services & Technology computing facilities, systems and resources applies to all members of the University community, including faculty, students, staff, contractors, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access service or eduroam access, and to those who register their computers and other devices through Conference Services programs or through other offices, for use of the campus network.

Policy Statement

These guidelines provide direction regarding the privacy, security, and integrity of West Chester University (WCU) data, especially confidential data, and the responsibilities of institutional units and individuals for such data. The guidelines provided herein apply to all WCU faculty, staff, students, visitors, and contractors.

This policy applies to all divisions and departments.

WCU maintains data essential to the performance of University business. All members of the University community have a responsibility to protect University data from unauthorized generation, access, modification,

disclosure, transmission, or destruction. The objective of these guidelines is to assist WCU employees and contractors in the assessment of data to determine the level of security which should be implemented to protect that data. This applies to paper and electronic copies where the data is stored. All data should be classified into three levels of security: Confidential, Sensitive, and Public. Once data has been classified, appropriate safeguards should be implemented to protect data from theft, loss, and/or unauthorized disclosure, use, access, and/ or destruction. Appropriate safeguards including encryption are found in related guidelines.

Although a large portion of WCU data is available for the public, some data have restrictions due to privacy protections mandated by federal, state, or local regulations and laws, ethical considerations, and proprietary worth. To comply with these mandates and protect the WCU community, WCU has the right and obligation to protect the confidentiality, integrity, and availability of data under its purview. Data can also be classified based on the application of the Right to Know Law. The classification level assigned to data will provide guidance to data custodians and others who may collect, process, or store data.

All members of the WCU community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by WCU, irrespective of the medium on which the data reside and regardless of format (such as in electronic, paper, or other physical form).

Policy Framework

University data should be classified into the appropriate category; Confidential, Sensitive, or Public. Data is defined as assets belonging to the University and should be classified according to the risks associated with the data being stored or processed. Confidential data requires the highest level of protection to prevent unauthorized disclosure or use. Data, which is sensitive or public, may be given proportionately less protection. Data is generally stored in collections (i.e., databases, files, tables, etc.) Often these collections do not segregate the more sensitive data elements of a collection from the less sensitive data. Therefore, in determining the classification category, the most sensitive data element in the collection should be used to classify the entire collection.

Examples of Confidential Data include data which includes PII (Personally Identifiable Information,) PHI (Protected Health Information), and data that is protected by federal, state, or local laws and regulations including but not limited to:

- Medical Records
- Disability Records
- Student Education Records that are directly related to prior, current, or prospective students but not including "directory information" such as a student's name, address, degrees, and awards subject to certain requirements specified in FERPA
- Student Financial Records
- Social Security Numbers or Partial Social Security Number
- Personnel and/or Payroll Records
- Law Enforcement and confidential investigation records
- Specific Donor Information

- Date of Birth
- Driver's License Number
- Citizenship or immigration status
- Information on facilities security systems
- Unpublished research data
- Privileged Legal Information
- Credit Card Information
- Passwords
- Personal Financial Information

Examples of Sensitive Data include:

• University Partner or Sponsor Information, where no more restrictive confidentiality agreement exists

• Certain Research Records

• Library and archive circulation and order transactions

Examples of Public Data include:

• General access data on WCU's website

• Approved official meeting minutes

• Published policies and documents

• Employment data to include name, position, compensation, employment contractor agreement and length of service

• Publicly posted press releases

• Directory Information under FERPA

• Publicly posted schedules of classes or course catalog

• Publicly posted interactive maps, newsletters, newspapers, job announcements, and magazines

Compliance

- Information Security Office will keep policy up to date and provide guidance to data owners on their classification processes and determinations.
- Data Owners will determine the classification of centralized databases.
- Users will determine the classification of the data within their responsibilities.

Policy Exceptions

All exemptions are approved by the Senior Associate Vice President & CIO of Information Services & Technology.

Procedures

WCU should implement appropriate managerial, operational, physical, and technical safeguards for access to, use of, transmission of, and disposal of University data. Confidential Data require the highest level of protection. If there is uncertainty regarding the category of the data, the higher level of safeguards should be applied.

General Safeguards for All Data

- All WCU data should be classified using the categories Confidential, Sensitive, or Public,
- Following initial classification, University data should remain classified at the initial level or reclassified as needed due to changes in usage, sensitivities, law, or other relevant circumstances.
- Data should be protected in accordance with the security controls specified for the classification level that it is assigned.

• The classification level and associated protection of replicated data should remain consistent with the original data [e.g. (i) confidential HR (Human Resources) data copied to removable media (e.g., flash drive), or from one server to another, retains its confidential classification; (ii) printed copies of Confidential Data is also confidential].

• Any physical or logical collection of data, stored, in transit, or during electronic transfer (e.g., file, database, emails and attachments, filing cabinet, backup media, electronic memory devices, sensitive operation logs, or configuration files) containing differing classification levels should be classified as a whole at the highest data classification level within the collection. Any data subset that has been separated from any such collection should be protected in accordance with the protection specified for the classification level of the data subset if assigned; otherwise, the data subset retains the classification level of the original collection and requires the same degree of protection.

• Destruction of data (electronic or physical) or systems storing data should be done in accordance with Records Retention and Asset Management policies and guidelines. Questions regarding best practices for destruction of data should be directed to the IS&T Help Desk.

•Before systems or media are reused or discarded, they must be sanitized according to NIST standards or physically destroyed. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf).

Safeguards for Confidential Data

- Must be protected to prevent loss, theft, unauthorized access, disclosure, modification, and/or destruction.
- Should be labeled Confidential Data.
- Confidential electronic data should be protected with strong passwords and stored on devices or in locations that are recommended by IS&T to have appropriate access controls and encryption measures.
- Confidential Data in transit will be encrypted, or subject to other appropriate security measures, to reasonably protect personally identifiable information. These measures ensure data transmitted over the Internet is not viewed or modified by unauthorized third parties.
- Confidential Data at rest will be encrypted, or subject to other appropriate security measures, to reasonably protect personally identifiable information. Servers, laptops, folders and/or individual files containing personally identifiable information will be encrypted to ensure data is not viewed or modified by unauthorized third parties.
- May only be disclosed on a strict need-to-know basis, within the course of legitimate business operations.
- Confidential physical data should be stored only in a locked drawer or room or an area where access is controlled using sufficient physical access control measures to detect and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

- When sent via fax, it should be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Should be properly destroyed when no longer needed in accordance with WCU and PASSHE (Pennsylvania State System of Higher Education) policies, retention schedules and Commonwealth and Federal statutes.

Safeguards for Credit Card Data

- All divisions that process or store cardholder data and have access to the information as a result of Internet, mail, fax, or telephone acceptance of credit card account information are required to comply with the American Express, Discover, VISA USA, and Master Card International operating regulations and the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is intended to protect cardholder data in the card-not-present industry. A card-not-present transaction can include Internet, mail, fax, or telephone acceptance of credit card account information.
- All third-party vendors that divisions use to fulfill PCI compliance will be retained at the division's expense.

Safeguards for Sensitive Data

- Should be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
- Should be stored in a controlled environment (e.g., file cabinet or office where physical controls are in place to prevent disclosure) when not in use.

- Should not be posted on any public website unless prior approval is given by external affairs and Office of Legal Counsel.
- Should be destroyed when no longer needed in accordance with the Records Retention and Asset Management policies and guidelines.

Safeguards for Public Data

Public data is available to external parties and the general public. Protection considerations should be applied to maintain data integrity and prevent unauthorized modification of such data. Safeguards for Public Data may include:

- Storage on an appropriately secured host.
- Appropriate protection against data integrity compromise.
- Redundant systems to maintain availability as appropriate.
- Retention according to public record requirements.
- Appropriate recovery plan.

Definitions

Confidential Data: Confidential data is considered the most sensitive and requires the highest level of protection. Confidential data include data that the University must keep private under federal, state, or local laws and regulations, or based on its proprietary worth. Confidential data may be disclosed to individuals on a strict need-to-know basis only, where the law permits.

Sensitive Data: Sensitive data is generally private to PASSHE. Access is limited to PASSHE community members on a need-to-know basis and these data are not generally available to external parties.

Public Data: Public Data has no legal or other restrictions on access or usage and may be open to the university community and the general public.

References

Acceptable Use Policy

Records Retention Policy

NIST 800-88 Rev 1
(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)

PCI-DSS: Requirements and Test Procedures Version 4.0
(https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf)

Student Privacy and FERPA Policy

Reviewed by: Information Services & Technology

Policy Owner: Stephen Safranek
Chief Information Security Officer
Information Services & Technology

Office of Labor Relations Review: Review completed December 27, 2022

Approved by:

JT Singh
Senior Associate VP & CIO
Information Services & Technology
Date: October 13, 2023

Effective Date: **October 13, 2023**

Next Review Date: October 13, 2027

History:

Initial Approval: 8/12/2014 - Deke Kassabian, VP of Information Services & Technology

Review Dates**:**

1/1/2014 – Reformatted to IS&T Policy Template
8/12/2014 – Reviewed and revised by CIO
8/20/2022- Reviewed and revised by CISO
10/26/2022 - Reviewed and revised by IS&T Senior Team
3/14/2023 - Revised to add information about encryption of confidential data
10/13/2023 - Revised for new signature and review date details

Amended: