PennWest
UNIVERSITY

Policy IT027: Data Classification Policy

Recommended for Approval by: Fawn R. Petrosky
Fawn Petrosky, Vice President for Finance

Approved by: Dale-Elizabeth Pehrsson
Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

This policy governs the privacy, security, and integrity of Pennsylvania Western University (PennWest) data, especially confidential data, and the responsibilities of institutional units and individuals for such data. The procedures provided herein apply to all Penn West University faculty, staff, students, visitors, and contractors.

PennWest University 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 this policy is to assist PennWest University employees and contractors in the assessment of data to determine the level of security, which must be implemented to protect that data. This applies to paper and electronic copy where the data is stored. All data is classified into three levels of security, Confidential, Sensitive, and Public. Once data has been classified, appropriate safeguards are implemented to protect data from theft, loss, and/or unauthorized disclosure, use, access, and/ or destruction. Appropriate safeguards including encryption are found in related policies.

Although a large portion of University 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 University community, PennWest University 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.

B. Definition(s)

• **Confidential Data:** Confidential data are considered the most sensitive and require 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 law permits.

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

• **Public Data:** Public Data have no legal or other restrictions on access or usage and may be open to the University community and the general public.

C. Policy

• Data Management

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

o Data Classification. The University must classify data into the appropriate category. Data are assets belonging to the University and should be classified according to the risks associated with the data being stored or processed. Confidential data require the highest level of protection to prevent unauthorized disclosure or use. Data, which are sensitive or public, may be given proportionately less protection. Data are 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 is used to classify the entire collection.

Examples of Confidential Data include:

- Medical Records
- Health Insurance Information
- Disability Records
- Student Records
- Student Conduct Records
- Social Security Numbers or Partial Social Security Numbers
- Personnel and/or Payroll Records
- Specific Donor Information
- Drivers License Number
- Privileged Legal Information
- Credit or Debit 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:

- Penn West University's website
- Financial transactions
- Approved official meeting minutes
- Official policies and documents
- Employment data to include name, position, compensation, employment contractor agreement and length of service
- Publicly posted press releases
- Publicly posted schedules of classes or course catalog
- Publicly posted interactive maps, newsletters, newspapers, job announcements, and magazines

• DATA SAFEGUARDS

Penn West University entities must 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. This policy provides examples of safeguards.

o General Safeguards for All Data

- Using the categories Confidential, Sensitive, or Public, all System data must be classified.

- Following initial classification, system data must remain classified at the initial level or reclassified as needed due to changes in usage, sensitivities, law or other relevant circumstances.

- Data must 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 must remain consistent with the original data [e.g. (i) confidential HR data copied to a CD-ROM, or other 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 must 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 must 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 must be done in accordance with Records Retention and Asset Management policies and procedures.

- Before systems or media are reused they should be wiped according to Department of Defense standards (http://www.dtic.mil/whs/directives/corres/html/522022m.htm) to ensure no residual data.

o **Safeguards for Confidential Data**

- Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.

- Must be labeled Confidential Data.

- When stored in an electronic format must be protected with strong passwords and encryption measures.

- May only be disclosed on a strict need-to-know basis and consistent with applicable policies and statutes.

- Must 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, must 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.

- Must be destroyed when no longer needed in accordance with System policies, procedures or statutes.
- Must not be electronically sent or stored using unapproved/personal 3rd party email, instant messaging, chat, text messaging, storage, etc.

- When transmitted in an electronic format must be protected with encryption measures.

- Users that handle Confidential Data on a regular basis will be subject to additional Security Awareness Training.

o **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.

- Comprehensive information on PCI requirements and merchant levels may be found on the PCI Security Standards Council Web site at the following link : https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

- Information on merchant levels, penalties for violation, and frequency of required security assessments is available at the following page on the Visa Web site: http://usa.visa.com/merchants/risk_management/cisp_merchants.html. All third party vendors that divisions use to fulfill PCI compliance will be retained at the division's expense.

- Storing cardholder data on local hard drives and removable electronic media is prohibited, unless explicitly authorized for a defined business need.

- Primary Account Numbers

  - May not be sent via messaging technologies such as email, instant messaging, chat, text messaging, etc.

- Users that handle credit card data must take PCI Security Awareness Training annually.

o Safeguards for Sensitive Data

- Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.

- Must be stored in a controlled environment (i.e. file cabinet or office where physical controls are in place to prevent disclosure) when not in use.

- Must not be posted on any public website unless prior approval is given by external affairs and Office of Legal Council.

- Must be destroyed when no longer needed in accordance with the System's Records Retention and Asset Management policies and procedures.

o Safeguards for Public Data

Public data are available to the 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 integrity protection.
- Redundant systems to maintain availability as appropriate.
- Retention according to public record requirements.
- Appropriate recovery plan.

D. Procedure(s)

Not Applicable.

E. Related policies

Credit Card Acceptance and Security Policy

F. Contact Information

Information Technology Services

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or Pennsylvania law would create the need for an immediate change.