



---

## Policy IT028: Information Security Awareness Policy

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

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

Effective Date: 2/24/2023

---

### A. Intent

The intent of this policy is to raise the awareness of information security, and to inform and highlight the responsibilities of faculty, staff, and student workers regarding their information security obligations. Formal information security awareness will aid in the protection of data, personal, intellectual property, financial, or restricted and sensitive information, networked systems, and applications entrusted to and utilized by Pennsylvania Western University (PennWest), by providing a broad understanding of information security threats, risks, and best practices. It is necessary to protect the confidentiality, integrity, and availability of University technology assets.

Technical IT security controls are a vital part of an information security framework- but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all workers, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks, which directly target humans rather than IT systems.

Lacking adequate information security awareness, workers are less likely to recognize or react appropriately to information security threats and incidents and are also more likely to place information in danger through ignorance and carelessness.

This policy applies to all faculty, staff, and student workers as they may access, store, process, transmit or manage University data, systems, or applications. As members of the PennWest community- faculty, staff, and student workers are accountable, and have an obligation to demonstrate an understanding of their unique role and responsibility as the best defense to ensure the protection of the University's information, data, and reputation.

## **B. Definition(s)**

- **Social Engineering** - is the art of manipulating people so they give up confidential information.
- **University Data** - University Data is any data or information that is created, owned, received, stored, or managed by PennWest.

## **C. Policy:**

The University Information Security & Technology Operations Office is responsible for the information security awareness program for the University. The program will include an enhanced understanding and appreciation of information risks; information about the threats, techniques, and consequences to the University; information on best practices; guidance on handling sensitive data and avoiding unintentional data exposure; information on recognizing and reporting incidents; guidance and resources to protect information and devices at work and at home.

### ***Faculty, Staff and Students:***

Formal participation and review of the security awareness program is mandatory for all faculty, staff, and students every year.

University Vice Presidents, Directors, and Deans are required to ensure adherence to the policy, and completion of the required program. Program content will be updated yearly to reflect current security trends, threats, techniques, business requirements, and the evolving environment of information security.

The Office of Human Resources will coordinate, monitor, and track the completion of the required Security Awareness program. University Vice Presidents, Directors, and Deans are required to ensure adherence to the policy, and completion of the required program. Program content will be updated yearly, in order to reflect current security trends, threats, techniques, business requirements, and the evolving environment of information security.

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems.

## **D. Procedure(s)**

Not applicable.

## **E. Related policies**

Not applicable.

## **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.