



# California University of Pennsylvania

## INFORMATION SECURITY AWARENESS POLICY

### A. Purpose & Scope:

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 the University, 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 vulnerable humans rather than IT and network 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 California University of Pennsylvania 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 California University of Pennsylvania.

### C. Policy/Procedure(s):

The University Technology Services' Networking and Security 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 reporting incidents; guidance and resources to protect information and devices at work and at home.

***Faculty, Staff and Student Workers:***

Formal participation and review of the security awareness program is mandatory for all full-time and part-time faculty and staff, every year. Newly hired faculty and staff are required to complete the training within thirty days of their hire date. Student workers who may have access to, or the ability to store, process, transmit or manage University Data are also required to complete this training within thirty days of their hire date. It is the responsibility of the student worker's supervisor to ensure that the student worker completes this requirement.

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. Effective date:** January 28, 2020

**Adopted:** January 28, 2020                      **by:** President's Cabinet

**Amended Date:**