Implementation Date: 02/04/22 Control Area: Personnel

Approval: Daniel Duncan Review Date: 04/03/22

Objective:

The Pennsylvania College of Technology will ensure the creation, maintenance, and implementation of a Security Awareness Training and Education program and will include setting guidelines, documentation, and security training requirements for use of college information systems and assets.

Purpose:

The Awareness Training and Education Program will ensure that the necessary requirements to improve the college’s security posture for the security and privacy of the college information systems, assets, and their environments are met including mandated role-based awareness training and continuous training with consideration towards the constant changes in the threats and vulnerabilities to the college systems.

Audience:

The CISO (Chief Information Security Officer) will work jointly with other qualified professionals such as the ISO (Information Security Officer), ITS (Information Technology Services) Staff, and Third-Party Vendors to ensure continued compliance with this policy. All persons or departments employed by the Pennsylvania College of Technology with access to the college’s information systems are subject to compliance with this policy.

Policy:

**AT-2: Literacy Training and Awareness**

The CISO will develop, implement, and maintain an Awareness Training and Education Program and will ensure the requirement of this training be provided to every user employed by the Pennsylvania College of Technology with access to its’ information system and information assets.

Basic expectations and outcomes of the Awareness Training and Education Program will include, but not limited to, security training with consideration to proper use of the information system, information assets, security of non-digital systems and assets, social engineering, phishing, spear phishing, etc.

**AT-3: Role-Based Training**

Individuals required to participate in the Awareness Training and Education Program training include, but not limited to, network administrators, system developers, ITS (information technology staff), and users employed by the college with access to its’ information system and assets.

Training will be provided for individuals with specific roles within the information system working with information systems and assets marked as critical or high-impact level of risk as described by the Media Protection Policy.

Awareness Training Education Program training will be provided to all new hires to the Pennsylvania College of Technology faculty and staff, when significant changes effect the college information system or its assets, upon request by college administration or its users, or annually at a minimum.

**AT-4: Training Records**

Documentation will be developed, implemented, and maintained to include records of all individual users, their roles, level of training completed, date of training, and administrator involved in the conduction of training. Documentation will be kept for record jointly by the CISO and college administration HR staff.

**AT-6: Training Feedback**

Documentation and records of training will be reviewed and assessed annually at a minimum jointly by the CISO and other qualified professionals including, but not limited to, the ISO, ITS, etc.

Awareness Training and Education will be tested using qualitative measures to produce baselines and benchmarking of training to identify risks and vulnerabilities to the college information systems and assets and will be included in the revisions and changes to the Awareness Training and Education Program.

Review and Update:

This policymust be reviewed at least once every three yearsand may be modified or discontinued as deemed necessary by the CISO. All revisions to this policy must be documented and maintained for review for a minimum of 5 years with disclosure of updates to all affected persons and departments as soon as reasonably possible.

Exceptions:

Requests forexceptions to this policy may be made to and will be reviewed for approval by the CISO with a record of all requests and approvals, including information for reasons for the exception, potential risks and benefits for the exception, and length of the expectation conducted and will be kept of record for a period of at least 5 years.

Documentation of all exceptions on record must be reasonably monitored, reviewed, and assessed to determine the continuation of an exception during the life of that exception and at the end of the approved exceptions life, the period of that exception’s retirement, or at a minimum of 3 years.

Disciplinary Action:

Instances of violation to this policy will be addressed in accordance with relevant HR policies, guidelines, and procedure. Sanctions will determine by the appropriate executive or administrative bodies including but not limited to termination or suspension from duties or employment by the college as described by the Pennsylvania College of Technology disciplinary procedures document.

References:

<https://www.pct.edu/student-life/student-policy/code-of-conduct>

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

<https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge>.

Definitions:

CISO (Chief Information Security Officer):

* The senior most level executive security professional within the organization of the Pennsylvania College of Technology responsible for the protection of the College’s information assets and programs.

Control:

- The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.

Incident:

- An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Assets:

* A body of information defined and managed as a single entity within the organization which may have financial value.

Information System:

* A system organized to collect, process, store, and distribute information including but not limited to computer systems, people, documents, and technology.

ISO (Information Security Officer):

* A security professional within the organization of the Pennsylvania College of Technology responsible for assisting the CISO with the protection of the College’s information assets and programs.

PII (Personal Identifiable Information)

* Any representation of information that allows for the identification of to whom the information applies to be reasonably inferred by either directly or indirectly.

Policy:

* A statement of intent provided to establish procedures and guidelines to direct decisions and actions of the College.

Risk

- The potential for loss or damage when a threat exploits a vulnerability.

Revision History:

04/03/22 – Policy Created and Implemented.