Implementation Date: *04/01/22* Control Area: *NIST SP800-53 R5:Program Management*

Approval: *Daniel Duncan* Review Date: *04/01/22*

Objective:

The program management plan will describe the Pennsylvania College of Technology’s security requirements and its expected outcomes to develop an information security program and will describe the program management controls and controls used or may be used to meet those requirements.

Purpose:

The program management plan will support the Pennsylvania College of Technology’s mission to provide an information security program to ensure the confidentiality, integrity, and availability of its used, stored, and accessed information media assets, systems, and their environments.

Audience:

The CISO (Chief Information Security Officer) will work jointly with the Pennsylvania College of Technology administrative staff and HR (Human Resources) staff 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 may be subject to compliance with this policy.

Policy:

**PM-2: Information Security Program Leadership Role**

A senior information security officer employed by the college will be referred to as CISO and will be assigned the authority and resources necessary to ensure an effective and successful development and implementation of an information security program.

**PM-3: Information Security and Privacy Resources**

The CISO will work jointly with the relevant Pennsylvania College of Technology administrative staff and HR staff to develop an inventory of required and necessary resources including budgets, staffing, assets, and protected media assets, and will appropriately assign those resources with documentation of classification, authorization, usage, and approval.

**PM-4: Plan of Action and Milestones Process**

The process for the creation of a plan of action and milestones for the information security program will be developed, maintained, and implemented by the CISO including details of the risks to current or future college information media and assets, and to college operations.

Review of this process should be conducted every four years at a minimum, or until significant changes to the information security program, college information systems, or their environments are made.

**PM-5: System Inventory**

The CISO will appoint an ISO or other qualified professions to develop and maintain an inventory of all college information systems and information assets will be developed and maintained annually at a minimum or when significant changes are made to the college information systems.

All PII stored and processed by the college will be assessed and marked appropriately annually at a minimum and will be sanitized as described in the Pennsylvania College of Technology Media Protection Police when deemed appropriate as described by the Personally Identifiable Information Policy.

**PM-6: Measure of Performance**

Outcome based performance metrics including baselines and benchmarking of the information security program will be recorded and documented to develop, monitor, and report on the performance of the information security program.

**PM-7: Enterprise Architecture**

The CISO will determine based on risk the use or maintenance of services on the college campus or off campus including services such as AWS (Amazon Web Services), Azur, or Google Cloud.

**PM-8: Critical Infrastructure Plan**

The CISO will work jointly with the Pennsylvania College of Technology Lead System Administrator to develop, implement, and maintain assets and resources critical to the storage and processing of critical assets. Critical college operations will be defined and documented in the information security program and will include protection strategies as described in the college Media Protection Policy.

**PM-9: Risk Management Strategy**

A comprehensive strategy managing risks to the college information assets, media, and operations including, but not limited to, instances involving PII, HIPAA, and FERPA records will be developed, maintained, and implemented. Reviews will be conducted annually at minimum or when significant changes are made to the college information media or assets, or to college operations.

**PM-10: Authorization Process**

Not Included.

**PM-11: Mission and Business Process Definition**

The ISO will work jointly with other qualified professionals to ensure the continuity and protection of college business operations, assets, and media by use of incident response and readiness methodologies as defined in the Incident Response Policy including the creation, use, and maintenance of backups with approval and documentation for review by the CISO.

**PM-12: Insider Threat Program**

Not Included.

**PM-13: Security and Privacy Workforce**

The Pennsylvania College of Technology will employ a Security Awareness Training and Education program as described by the Awareness Training Policy.

**PM-14: Testing, Training, and Monitoring**

The CISO will ensure the development, implementation, and use of the Awareness Training Policy including assessment, monitoring, and review of the effectiveness of the training and make changes when necessary as described by the Awareness Training Policy.

**PM-15: Security and Privacy Groups and Associations**

The CISO will provide ongoing security awareness and privacy education to faculty, staff, and departments employed by the Pennsylvania College of Technology with access to its’ information system including webinars, conferences, etc. and will associate other college’s including Lock Haven University, Lycoming College, etc. and other security groups on the topics of potential risks and threats to the college.

**PM-16: Threat Awareness Program**

Not Included.

**PM-17: Protecting Controlled Unclassified Information on External Systems**

The CISO will work jointly with the Pennsylvania College of Technology network administrators to determine the use, storage, and access of controlled media assets to ensure privacy and proper authorization as described by the Media Protection Policy.

**PM-18: Privacy Program Plan**

The CISO will work jointly with the Pennsylvania College of Technology Administration to develop a plan of action to appropriately the handling of confidential or protected information including FERPA, HIPAA, etc. as described by the Personally Identifiable Information Policy.

The Pennsylvania College of Technology Administration will assign an administrative position to oversee the privacy program plan and ensure compliance with federal, local, and state laws and regulations regarding instances of all relevant violations.

**PM-19: Privacy Program Leadership Role**

Not Included.

**PM-20: Dissemination of Privacy Information**

Not Included.

**PM-21: Accounting of Disclosure**

Not Included.

**PM-22: Personally Identifiable Information Quality Management**

Not Included.

**PM-23: Data Governance Body**

The CISO will review, and update policies as described by the individual policies as published and will review documentation regarding retention and classification of data to ensure appropriate use, storage, and access of data.

**PM-24: Data Integrity Board**

Not Included. (We will not need to compare our matchups to other college organizations, the breadth of information collected regarding comparison for use for the purposes of grants is not necessary enough for use of a data integrity board.)

**PM-25: Minimization of Personally Identifiable Information Used in Testing, Training, and Research**

Not Included.

**PM-26: Complaint Management**

The CISO will work jointly with the Pennsylvania College of Technology administration HR department to develop, implement, and maintain a process for receiving and managing complain, concerns, or questions from individuals about college security and privacy practices.

**PM-27: Privacy Reporting**

Not Included.

**PM-28: Risk Framing**

The CISO will work jointly with the ISO, ITS (Information Technology Staff), or other qualified professionals to define, describe, and review risk and vulnerability to the Pennsylvania College of Technology information systems, assets, protected media assets, and their environments as described by the Risk Analysis Policy.

**PM-29: Risk Management Program Leadership Roles**

Not Included.

**PM-30: Supply Chain Risk Management Strategy**

Not Included.

**PM-31: Continuous Monitoring Strategy**

The CISO will appoint the ISO, ITS, or other qualified professional staff to regularly monitor the security of the Pennsylvania College of Technology information systems including system updating, media storage assessment, and closed-circuit security cameras, etc. with documentation recorded and approved by the CISO including details of affected media, changes or updates, dates, and individuals or departments involved.

**PM-32: Purposing**

The CISO will work jointly with the ISO, ITS, or other qualified professional staff to assess and review the Pennsylvania College of Technology information systems, media assets, and their environments to ensure use is consistent with intended purposes as described by the Risk Analysis Policy.

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:

*04/01/22 – Policy Created and Implemented.*