Implementation Date: *03/3/2022* Control Area: NIST SP800-53 R5: CA

Approval: *Daniel Duncan* Review Date: *04/17/2022*

Objective:

The assessment, authorization, and monitoring strategy will be developed, maintained, and implemented to include detailed assessment of the Pennsylvania College of Technology information systems, components, documentation, security and privacy methodologies, policies, risks, and vulnerabilities.

Purpose:

The security assessment, authorization, and monitoring strategy will ensure that the necessary procedures and guidelines are used to meet with the security requirements of the college information systems. This strategy will ensure an acceptable level of risk is maintained in the college operations, functions, and 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), 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:

**CA-2: Control Assessments**

The CISO will determine the type of assessment to be conducted and the appropriate person or team to conduct the assessment. The conduction of a control assessment may be designated to the employment of a public or private independent assessor or independent team of assessors with the intention of impartial conduction of an assessment at the approval of the CISO.

The control assessment plan will include the controls or control enhancements that will be assessed, the procedures used to determine control effectiveness, and the environment of, the team conducting, and roles and responsibilities associated with the assessment.

Specialized Control Assessment plans that include the verification and validation of system monitoring, insider threat assessment, malicious user testing, or other forms of testing must be developed and conducted to meet compliance with any applicable Federal, State, and Local laws and regulations and to meet compliance with the College’s security procedures for the protection of the College’s information assets.

The CISO will conduct or authorize a person or persons to conduct a review of and submit for approval the control assessment plan prior to the conduction of the assessment.

The review and approval of the control assessment plan will be documented with details of the extent that the controls assessed are implemented correctly, are operating as intended, and the outcome of the controls assessed are being met under the intended conditions set by the College’s established security and privacy requirements.

The results of the control assessment plan will be documented into a control assessment report containing information regarding correctness, effectiveness, and relevancy of controls assessed with recommendations for modification, alteration, or retirement of assessed controls. This control assessment report may include references to external organizations control assessments of relevant control assessment with the details of reasoning for comparison and use.

The control assessment report will be recorded and submitted to the CISO for review, approval, and documentation.

**CA-3: Information Exchange**

The CISO and College Administration will approve and manage the exchange of information between two or more systems using information security, data exchange, and data storage agreements accepted by the users of the Pennsylvania College of Technology information assets and services.

The information management and exchange agreements required for agreement by users will be determined and selected for use by the CISO and College Administration based on the factors of the impact level of the information exchanged or accessed, the relationship of the organizations involved in the exchange or access of information, or by the level of access to a college system by a user of another system. These information management and exchange agreements will be incorporated as formal contracts when appropriate, including instances of information management and exchange

The documentation of these information management and exchange agreements will include, as part of each information management and exchange agreement, the security and privacy requirements, the responsibility of each system, the impact level of the information communicated, and a review and update to these agreements.

Verification and prerequisite authorization by individuals or systems between two or more systems on the or between the Pennsylvania College of Technology to an external system is required prior to the acceptance of the transferal of data. Acceptance of the transferal of data will be determined by the identification of the information exchange as defined by the CISO and College Administrations approval and management of the exchange of information. Action or preventative measures will be taken to cease the transferal of data between systems if identification of systems involved with the transit of data can not be verified or validated.

**CA-5: Plan of Action and Milestones**

The ISO is responsible for the creation and documentation of a plan of action and milestones for remedial actions to be submitted and documented for approval by the CISO and College Administration to correct weakness or deficiency noted within the control assessment report documented during assessment of controls and control enhancements and will update existing plans of action and milestones at a minimum of 3 months based on the findings of the documented control assessment report, independent audits or reviews, and continuous monitoring activities. to reduce or eliminate known vulnerabilities in effected systems.

The ISO will use automated tools to maintain a system of accuracy, currency, and availability of the plan of action and milestones and develop a system to coordinate the disclosure of security and privacy information throughout the organization to ensure appropriate resources are available and directed to the necessary system vulnerabilities effectively.

**CA-6: Authorization**

The CISO will work jointly with the HR (Human Resources) department head and with another qualified professional such as the ISO to determine authorization, common controls, and the explicit acceptance of risk to the college operations, information systems, and assets.

The CISO will work jointly with the HR department head and with another qualified professional such as the ISO to update authorizations when necessary. Updates to authorization will be recorded and include documentation with details of affected authorizations, purpose, dates of revision and implementation, and effected systems, controls, and control enhancements.

**CA-7: Continuous Monitoring**

The ISO will develop and implement a strategy to assess and monitor controls and risks to the Pennsylvania College of Technology systems at a frequency and scope deemed necessary by and to support risk-based decisions as determined by and approved and documented by the CISO.

The continuous monitoring strategy will:

* Determine and document correlations and analysis of the results ongoing control assessments, all ongoing monitoring of the College systems as prescribed by the CISO and as defined as critical by the College’s security posture and security procedures and will include response actions to mediate vulnerabilities found within the control assessment report.
* Employ a system to effectively collect empirical data to determine and document the need for modification of this strategy by analyzing trends of frequency of and types of continuous monitoring activities used.
* Include risk monitoring directed by a risk tolerance profile of the College information systems and information assets documented, reviewed, and approved by the CISO, will determine the effectiveness of current implementation risk response measures, will monitor compliance of, and verification of implemented required risk response measures, and security and privacy requirements.
* Identify changes to the College systems and operational environments that may effect security and privacy risks.
* Include testing, monitoring, and analysis of implemented controls to evaluate and mediate inconsistencies, discoordination, and interference.
* Include automated tools to develop a system to document and maintain accuracy, currency, and availability of information collected with intention to improve ongoing awareness of the College security and privacy posture to support College risk management decisions.
* Include details of the security and privacy status of the monitored College systems and will be reported to the CISO and College Administration for review and approval.

**CA-8: Penetration Testing**

The CISO will designate a qualified and professional such as the ISO, ITS, or third-party vendor to conduct penetration testing on the College information system assets and system components virtually and at physical access points as deemed necessary by, and at a frequency deemed necessary by the continuous monitoring strategy and will record and document vulnerabilities and risks to those assets and components.

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:

*04/17/22 – Policy Created and Implemented.*