Implementation Date: *02/18/2022* Control Area: *NIST SP800-53 R5: Risk Assessment*

Approval: *Daniel Duncan* Review Date: *04/22/2022*

Objective:

The controls listed within this document will describe the Pennsylvania College of Technology’s security posture to ensure that the College is to adopt procedures for the security of the College’s information assets, develop a risk assessment strategy, and assign responsibilities for the College’s continued compliance with this policy.

Purpose:

The assessment of threats to the confidentiality, integrity, and availability of the College’s Information Assets through Risk Assessment and Risk Tolerance is necessary for the protection of these Information Assets to ensure the responses are appropriately consolidated.

Audience:

This policy is in effect for and applies to all persons employed by, or on behalf of the Pennsylvania College of Technology who hold the positions of CISO (Chief Information Security Officer) and ISO (Information Security Officer) and persons have been selected and documented for approval to perform the responsibilities listed within this policy by the CISO.

Policy:

**RA-2: Security Categorization**

The categorization and assessment of security must describe the potential of impacts and consequences to the loss of Confidentiality, Integrity, and Availability to the Pennsylvania College of Technologies information systems’ operations and information assets and these information systems, information assets, a mapping of the components where their information is stored, processed, and transmitted, must be defined, categorized.

These information systems, information assets, and components must be assigned an impact-level defined and documented for approval by and kept for record by the CISO.

**RA-3: Risk Assessment**

The conduction of a risk assessment must identify threats and vulnerabilities in the College information system and to the College information assets including but not limited to the determination of the likelihood and magnitude of the impacts and consequences to the loss of Confidentiality, Integrity, and Availability of these systems, assets, their components, and determine the likelihood and consequence that may result in the processing of PII (personally identifiable information) and information protected by Federal, State, and local laws and regulations.

The decisions made to manage the identified risks found from the results of the risk assessment must be aligned with the mission or business process of the Pennsylvania College of Technology.

The results of a risk assessment must be documented in a risk assessment report and kept for record by the CISO for a minimum of 5 years.

The results of a risk assessment must be reviewed by the CISO or by persons designated by the CISO within 30 days of the documentation of the results and again within 90 days of the next risk assessments conducted for a minimum of 5 years.

Updates or modification of a risk assessment must be made when there are changes made to an information system or systems, their environments of operation, or when any conditions change that impact the security of or privacy of these systems or environments that are deemed necessary by the CISO.

The results of the risk assessment and all modifications made to the risk assessment must be reported to the CISO and to the College Administrators overseeing the CISO and the Information Technologies department at Pennsylvania College of Technology.

**RA-5: Vulnerability Monitoring and Scanning**

Monitoring and scanning for vulnerabilities within the information system and applications hosted by the Pennsylvania College of Technology must be performed at a minimum, annually within 60 days of the last scan or within 14 days of any changes made to an information system or systems, their environments of operation, or when any conditions change that impact the security or privacy of these systems or environments that are deemed necessary by the CISO with all reports of any instances of all new vulnerabilities submitted and reviewed by the CISO or any persons designated by the CISO.

Vulnerability monitoring and scanning tools and techniques must include interoperability between tools and automation of those tools used and perform processes including but not limited to standards for enumerating platforms, detection of vulnerabilities and flaws of software used on the colleges information systems and detection of improper configuration of those systems, test procedures and measures of impact from vulnerabilities.

Review and assessment of risks found within the vulnerability monitoring and scanning reports and results must be conducted at a minimum of within 14 days of the instance of vulnerability monitoring and scanning results received.

Vulnerabilities and risks identified by the review of the vulnerability monitoring and scanning report must be remediated if the vulnerability or risk is deemed by the CISO, based on the defined impact-level threshold, as significant and must be remediated as soon as feasibly possible.

The results of the vulnerability monitoring and scanning report must be reported to the CISO and to the College Administrators overseeing the CISO and the Information Technologies department at Pennsylvania College of Technology to be distributed as deemed necessary by the CISO.

Updates and modifications must be made to the vulnerability monitoring and scanning tools and techniques to include the capacity to be readily updated and modified to meet demands of current vulnerabilities and risks found within the college information systems.

**RA-7: Risk Response**

The CISO or any persons assigned by the CISO must respond to vulnerabilities and risks to the Pennsylvania College of Technology information systems and information assets, and their components, if deemed appropriate by the established impact-level threshold. This must be done as needed appropriate by the CISO using, but not limited to, generating a plan of action to fix the vulnerability, or accept or reject the risk and must be aligned with the mission or business process of the Pennsylvania College of Technology.

**RA-8: Privacy Impact Assessments**

The CISO will conduct a privacy impact assessment for the Pennsylvania College of Technology information systems, programs, or other activities before the development of the collection of new information technology that processes, stores, or transmits PII virtually or physically to maintain compliance with Federal, State, and local laws and regulations.

Review and Update:

This policy, at a minimum of 3 years, must be reviewed by and 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.

Exceptions:

Requests for exceptions may be made to this policy with information including reasons for the exception, potential risks and benefits for the exception, and length of the expectation may be approved after review and approval by the CISO with a record of all requests and approvals with information of these exceptions including reasons for the exception, potential risks and benefits for the exception, and length of the expectation kept for a minimum of 5 years after the time of review.

Reviews of all exceptions on record must be reviewed and assessed for continued exception at the end of the approved exceptions life or at a minimum of 5 years.

Disciplinary Action:

The CISO is authorized to manage the Pennsylvania College of Technology’s network and information system and may act in the interest of the college and its information assets and information systems to, but not limited to, limit connection of or disconnect any user from them as deemed necessary by the Pennsylvania College of Technology policies and regulations, and to maintain compliance with federal, state, and local laws and regulations. Non-compliance with this policy may, at the discretion of the College, result in administrative action taken by the College.

References:

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

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

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.

CPE (Common Platform Enumeration)

* Standardized method of describing and identifying classes of applications, operating systems, and hardware on the Pennsylvania College of Technologies computing assets.

Impact-Level

* The sensitivity of information stored or processed on the Pennsylvania College of Technology computing assets and the potential impact from an event that results loss of the confidentiality, integrity, and availability of that information.

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:

*2/18/2022 – Policy Created and Implemented.*