Implementation Date: *03/13/22* Control Area: *PII Processing and Transparency*

Approval: *Daniel Duncan* Review Date: *05/01/22*

Objective:

A PII (Personally Identifiable Information) plan will be developed, implemented, and maintained to define information assets including physical and digital media that contain PII information such as SSN (Social Security Number), addresses, phone numbers, college ID number, email addresses, name, etc. and the methodologies employed to ensure privacy and security of this information.

Purpose:

The PII plan will define the colleges’ physical and digital media assets containing PII and the procedures and guidelines employed to protect them to improve the Pennsylvania College of Technology’s security of its storage and use of PII.

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:

**PT-2: Authority to Process Personally Identifiable Information**

The CISO will work jointly with the Pennsylvania College of Technology administration’s legal department to ensure PII and the systems and media used for access and storage is defined and assigned an impact-level for risk to the organization as described by the Pennsylvania College of Technology Risk Analysis Policy. The CISO will update, implement, or modify authorization and verification systems used by the college as necessary.

Documentation of impact-level and restrictions will be recorded with necessary information including authorities involved, impact-levels of risk, restriction of access, authorizations granted, and types of verification used.

**PT-3: Personally Identifiable Information Processing Purposes**

The CISO will work jointly with the Pennsylvania College of Technology administration’s legal department to define and document PII including the reasons for its’ creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal.

Identification, purpose, and documentation of these definitions will ensure owners and operators of the college systems and individuals whose information is processed by these systems will have an appropriate level of disclosure and understanding of how PII will be processed.

PII will be restricted for use only when compatible with college systems and when compliant to the purpose defined by the CISO and the Pennsylvania College of Technology administration’s legal department.

The CISO will monitor changes to the processing of PII and may implement interoperable automated systems to monitor these changes to ensure that these changes are made in compliance with Federal, State, and local laws and regulations, and improve the security and privacy of PII.

**PT-5: Privacy Notice**

The CISO will work jointly with the Pennsylvania College of Technology administration’s legal department to develop and implement privacy notices that will be provided to individuals annually at a minimum about the processing of PII

* when individuals initially begin contract with or establish relationship with the Pennsylvania College of Technology, when changes to the processing of PII are made, or before any instance occurs that requires processing of their PII
* is worded in a clear and easy to understand format including appropriate information about the processing of PII
* authorizes the processing of, and to the authority of, their PII
* identifies purpose of the processing of their PII
* may include all relevant information regarding consent and purpose as defined by the CISO and the Pennsylvania College of Technology
* will include information explaining what will occur if consent is declined
* will be collected and documented for record by the CISO to maintain compliance with Federal, State, and local laws and regulations

**PT-7: Specific Categories of Personally Identifiable Information**

The CISO will work jointly with the Pennsylvania College of Technology administration’s legal department to identify and define conditions or protections necessary for specific categories of PII which may be required by Federal, State, or local laws and regulations or by results of risk assessments that determine specific categories of PII that proposes a high level of risk.

Specific categories of PII that propose a high level of risk as described by the Pennsylvania College of Technology Risk Analysis Policy including social security numbers or information that describes an individual’s expression of their first amendment rights.

The CISO will develop and implement strategies to eliminate unnecessary collection, maintenance, and use of PII with a high level of risk and will explore alternatives to their use as a personal identifier.

The Pennsylvania College of Technology and its systems will not

* deny any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose their social security number
* and inform any individual who is asked to disclose their social security number, by what statutory or other authority such number is solicited, and what uses will be made of it

**PT-8: Computer Matching Requirements**

The CISO on behalf of the Pennsylvania College of Technology will obtain approval from the Data Integrity Board to conduct a matching program and when a college system processes information for the purpose of conducting a matching program will

* develop and enter a computer matching program
* publish a matching notice in the Federal Register
* Independently verify the information produced by the matching program before taking adverse action against an individual if required
* and provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual

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:

*05/01/22 – Policy Modified*