Implementation Date: *03/05/22* Control Area: NIST SP800-53 R5: Media Protection

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

Objective:

A media protection plan will be developed, implemented, and maintained to define the authorization of access, modification, and storage of the Pennsylvania College of Technology protected and private information assets and will describe appropriate sanitization of these assets prior to disposal or reuse.

Purpose:

The media protection plan will ensure that the colleges’ protected and private information assets are protected from unauthorized access, disclosure, or loss. Controlling access to college information assets to authorized users, and implementing procedures for asset handling, will improve the privacy and security of college information assets.

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:

**MP-2: Media Access**

The Pennsylvania College of Technology will restrict access to media including, but not limited to, laptops, portable devices, media removed from systems, physical files, etc. with protected or confidential information such as PII, HIPAA, or FERPA to persons, departments, or systems with appropriate permissions and authorizations.

**MP-4: Media Storage**

The Pennsylvania College of Technology will ensure that its protected and confidential digital and non-digital media assets are securely stored and physically controlled including the use of secure storage containers, conducting regular inventory checks, and engaging in consistent use of procedures to monitor, track, and store its media.

Protected and confidential digital and non-digital media assets will be safeguarded until their destruction or sanitization using approved equipment, techniques, and procedures are used to retire them as described in MP-6: Media Sanitization.

**MP-5: Media Transport**

Protected and confidential digital and non-digital media assets will be protected during transportation or transmission outside of secure environments and will meet compliance with the appropriate and relevant procedures deployed by the Pennsylvania College of Technology and federal, state, and local laws and regulations.

Monitoring, tracking, and secure storage of protected and confidential digital and non-digital media assets in transport will be ensured by persons, departments, or systems involved in the transportation of these media assets.

Activities associated with the transportation will be documented including information of persons, departments, the systems involved, and tracking and delivery records to prevent or detect loss, destruction, or tampering of these media assets.

Persons, departments, or systems involved in the transportation of protected and confidential digital and non-digital media assets will meet required authorization to conduct activities associated with handling and transport of those media assets.

**MP-6: Media Sanitization**

Protected and confidential digital and non-digital media assets will be sanitized prior to their disposal, release from the control of the Pennsylvania College of Technology, or release for reuse. This is accomplished when the original data is irretrievable from the sanitized media including, but not limited to, the use of media overwrites, factory resets, cross cut shredding of paper media, or digital media shredding.

The CISO will review, approve, and document media sanitization to ensure the verification of the effective destruction or sanitization of effected media assets and include record of actions and personnel involved, types of media, information stored, and date and time.

The CISO will assign qualified and authorized personnel to test equipment and procedures, at minimum of a 1 year or verification of effective media sanitization cannot be approved, to ensure intended sanitization conditions are satisfied.

Media assets obtained by the Pennsylvania College of Technology for reuse such as external hard drives, DVDs, tapes, flash drives, and memory cards will be sanitized without physical destruction to ensure malicious code or damage does not occur on the college systems prior to use.

The Pennsylvania College of Technology will develop and implement procedures to effectively purge or delete information remotely from protected and confidential digital media assets when those assets fall outside of the control and protection of the college and are accessible to unauthorized persons. The CISO will ensure the review, update, and use of these procedures.

**MP-7: Media Use**

Authorization and verification are required to access protected and confidential digital and non-digital media assets and their stored information during sanitation or configuration.

The CISO will develop and regularly monitor, review, or assign scope of permissions or clearances to handle private and protected media assets and will manage and document contracts and agreements required prior to access.

Authorization, verification, and tracking of portable storage devices used on the Pennsylvania College of Technology will be documented including details of ownership, and device capability and specification to reduce risks of use by assigning responsibility of addressing known vulnerabilities of these devices.

The Pennsylvania College of Technology will prohibit use of sanitization-resistant media by its staff, faculty, and departments to store protected and confidential information.

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.*