Implementation Date: *03/04/22* Control Area: NIST-800 53 R5: Access Control

Approval: *Daniel Duncan* Review Date: *05/1/22*

Objective:

An access control plan will be developed, implemented, and maintained to control access and use of the Pennsylvania College of Technology information systems and assets through assignment and verification of authorization of these systems and assets

Purpose:

The access control plan will authenticate access and use of the college information systems and assets by ensuring the necessary verification and authorization of its’ users to improve the privacy and security of the college information systems and 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:

**AC-2: Account Management**

The CISO will work jointly with other qualified professionals such as the ISO, ITS, or third-party vendors to establish account management roles, responsibilities, and permissions for individuals, departments, and groups as necessary to accomplish their designated function as described by their official job titles.

Account management roles, responsibilities, and permissions may include:

* Authorization and access to information systems and assets
* Creation, enabling, modification, disabling, or removal of accounts
* Monitoring of the use of accounts
* Notifying users when changes are made to their account including changes to their role, responsibilities, or permissions
* Other account management roles, responsibilities, or permission assignment or management as necessary

**AC-4: Information Flow Enforcement**

The CISO will work jointly with other qualified professionals such as the ISO, ITS, or third-party vendors to establish mechanisms for the control of information assets internally and externally on the college network and systems, and internet. Information flow enforcement will ensure approved authorization of access and use of college information assets by regulating the transfer of information assets to prevent access by unauthorized individuals or systems.

Mechanisms of information flow enforcement will compare security attributes of information assets and systems and will generate an appropriate response such as blocking or quarantining transfer, and alerting an appropriate system administrator as described by AC-2: Account Management.

**AC-7: Unsuccessful Logon Attempts**

Unsuccessful logon attempts by users will result in a 15-minute logon prevention lock after 3 failed attempts during a 5-minute period. When a maximum of 9 failed attempts is reached within a 60-minute period a lock of the account or node will be enforced until a system administrator initiates a release of the affected account or node.

**AC-11: Device Lock**

Device locking and session termination mechanisms will be implemented to college information assets and account management accounts to prevent unauthorized access to college information systems, assets, or accounts during periods of inactivity or unattendance by authorized entities.

Device locking and session termination mechanisms will initiate during periods deemed necessary by the CISO using the Pennsylvania College of Technology Media Protection and Risk Analysis policies described risk and risk handling.

**AC-22: Publicly Accessible Content**

Account management roles with authorizations, responsibilities, and permissions to publish publicly accessible information will receive appropriate training and education as described by the Pennsylvania College of Technology Awareness Training and Education Policy including training on information that is permissible and non-permissible for public access.

Account management roles with authorizations, responsibilities, and permissions to publish publicly accessible information will review publications before publishment to ensure protected and private information is not disclosed to unauthorized entities and will remove such information when discovered.

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.*