|  |
| --- |
| Pennsylvania College of Technology |
| Policy Portfolio |
| Security Privacy Controls – NIST SP 800-53 R5 |

|  |
| --- |
| Daniel Duncan  5-3-2022 |

***Index***

**Awareness Training and Education**………………………………………………………………………………………………………**1**

**Risk Assessment**……………………………………………………………………………………………………………………………………**3**

**Assessment, Authorization, and Monitoring**.……………………………………………………………………………………….**6**

**Media Protection**………………………………………………………………………………………………………………………………….**10**

**Access Control**………………………………………………………………………………………………………………………………………**13**

**Personally Identifiable Information**……………………………………………………………………………………………………..**16**

**Incident Response**………………………………………………………………………………………………………………………………..**19**

**Program Management**………………………………………………………………………………………………………………………….**23**

**Audit and Accountability**………………………………………………………………………………………………………………………**27**

**Contingency Planning**……………………………………………………………………………………………………………………………**30**

**Secure Software Development**……………………………………………………………………………………………………………..**33**

**Definitions**…………………………………………………………………………………………………………………………………………….**36**

**Control Exclusions**……………………………………………………………………………………………………………………………………………..**39**

AT Exclusions…………………………………………………………………………………………………………………………….**39**

RA Exclusions…………………………………………………………………………………………………………………………….**39**

AC Exclusions…………………………………………………………………………………………………………………………….**39**

PT Exclusions…………………………………………………………………………………………………………………………….**41**

PM Exclusions…………………………………………………………………………….…………………………………………….**41**

AU Exclusions………………………………………………………………..………………………………………………………….**42**

CP Exclusions…………………………………………………………………………………………………………………………….**43**

Implementation Date: 02/04/22 Control Area: NIST-800 53 R5: AT

Approval: Daniel Duncan Review Date: 04/03/22

Objective:

The Pennsylvania College of Technology will ensure the creation, maintenance, and implementation of a Security Awareness Training and Education program and will include setting guidelines, documentation, and security training requirements for use of college information systems and assets.

Purpose:

The Awareness Training and Education Program will ensure that the necessary requirements to improve the college’s security posture for the security and privacy of the college information systems, assets, and their environments are met including mandated role-based awareness training and continuous training with consideration towards the constant changes in the threats and vulnerabilities to the college 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:

**AT-2: Literacy Training and Awareness**

The CISO will develop, implement, and maintain an Awareness Training and Education Program and will ensure the requirement of this training be provided to every user employed by the Pennsylvania College of Technology with access to its’ information system and information assets.

Basic expectations and outcomes of the Awareness Training and Education Program will include, but not limited to, security training with consideration to proper use of the information system, information assets, security of non-digital systems and assets, social engineering, phishing, spear phishing, etc.

**AT-3: Role-Based Training**

Individuals required to participate in the Awareness Training and Education Program training include, but not limited to, network administrators, system developers, ITS (information technology staff), and users employed by the college with access to its’ information system and assets.

Training will be provided for individuals with specific roles within the information system working with information systems and assets marked as critical or high-impact level of risk as described by the Media Protection Policy.

Awareness Training Education Program training will be provided to all new hires to the Pennsylvania College of Technology faculty and staff, when significant changes effect the college information system or its assets, upon request by college administration or its users, or annually at a minimum.

**AT-4: Training Records**

Documentation will be developed, implemented, and maintained to include records of all individual users, their roles, level of training completed, date of training, and administrator involved in the conduction of training. Documentation will be kept for record jointly by the CISO and college administration HR staff.

**AT-6: Training Feedback**

Documentation and records of training will be reviewed and assessed annually at a minimum jointly by the CISO and other qualified professionals including, but not limited to, the ISO, ITS, etc.

Awareness Training and Education will be tested using qualitative measures to produce baselines and benchmarking of training to identify risks and vulnerabilities to the college information systems and assets and will be included in the revisions and changes to the Awareness Training and Education Program.

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>.

Revision History:

04/03/22 – Policy Modified

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

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:

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:

**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 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>

Revision History:

*4/22/2022 – Policy Modified*

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>

Revision History:

*04/17/22 – Policy Modified*

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

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>

Revision History:

*05/01/22 – Policy Modified*

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

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>

Revision History:

*05/01/22 – Policy Modified*

Implementation Date: *03/13/22* Control Area: NIST-800 53 R5: PT

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>

Revision History:

*05/01/22 – Policy Modified*

Implementation Date: *03/25/22* Control Area: NIST SP800-53 R5: IR

Approval: *Daniel Duncan* Review Date: *05/03/22*

Objective:

The Pennsylvania College of Technology will ensure the creation and maintenance of an incident response plan including ATE (Awareness Training and Education), incident processing, and incident reporting for the college information system and will set guidelines and minimum expectations for the process of handling incident response.

Purpose:

The Pennsylvania College of Technology will properly management, and effectively use incident response plans to contain the scope of its incidents, reduce risk to the college information systems and informational assets, and return its affected systems to a state of intended operation as quickly as possible.

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:

**IR-2: Incident Response Training**

The Pennsylvania College of Technology will provide incident response training and awareness training to the administrators and users of the college’s information systems as appropriate for their roles and responsibilities in the incident response plan.

Incident response training and awareness training will be conducted prior to the changing of, or the assignment of roles or responsibilities to an individual or department in the incident response process. Additional training will be conducted prior to changes to an information system or its environment as necessary and will be conducted annually at a minimum.

Incident response training and awareness training will include identification and reporting of suspicious activities from internal and external factors.

A record will be kept of all incident response training and awareness training including all attending personnel, information systems, types/levels of training, and completion date.

**IR-3: Incident Response Testing**

The incident response plan will include review of potential incidents to the college information systems, assess incident response effectiveness, and identify potential weakness or deficiencies.

Testing may include checklists, walk-throughs, exercises, or simulations and will use qualitative and quantitative data aids to support the determination the effectiveness of the incident response process.

Testing will be conducted prior to any considerable changes to the college information system or its environment and will be conducted annually at a minimum.

**IR-4: Incident Handling**

The incident response handling will include the implementation of incident handling procedures including preparation, detection and analysis, containment, eradication, and recovery with additional consideration towards essential business functions and their associated incident response requirements.

A timeline for completion of the procedures of incident handling will be established and assigned to a qualified person or department by the CISO. In the event of the loss of protected media assets or the denial of essential college systems, the timeline for completion should be considered critical.

Incident handling procedures will work in conjunction with contingency planning procedures and will identify and record necessary information towards the improvement of these procedures and their respective training procedures.

**IR-5: Incident Monitoring**

Incident monitoring will be performed by the CISO or a designated incident response team personnel or department who may include the use of automated tracking, data collection, and analysis using systems such as Computer Incident Response Centers or other databases of incidents and network monitoring systems.

Incidents that occur within the college information systems or their environments will be monitored until the appropriate incident handling procedures have been effectively administered.

Incidents will be documented and recorded including details of the information system or environment affected, status of the incident, damage assessment, incident handling procedures used, information ascertained for use towards improvement of procedures and training, and all necessary information for forensic evaluation.

**IR-6: Incident Reporting**

Personnel are required to report suspected incidents to the CISO or college incident response team by the end of the workday upon discovery.

Suspected incidents that may result in violation of federal, state, or local laws and regulations including violations of FERPA (Federal Education Rights and Privacy Act), HIIPA (Health Insurance Portability and Accountability Act), or any incident involving PII, or the confidentiality, integrity, or authorization of the college systems must be reported immediately or as soon as possible.

**IR-7: Incident Response Assistance**

The CISO will work jointly with the college ITS to develop and implement support resources.

Support resources will include systems to offer advice and assistance to users with incident response roles and responsibilities of the college systems for the handling and reporting of incidents.

**IR-8: Incident Response Plan**

The Pennsylvania College of Technology will develop and implement an incident response plan to include:

* A guide for the implementation of incident response procedures.
* A description of the structure and organization of the incident response procedures.
* Provision of a high-level approach as the incident response procedures applies to the college.
* Definitions of reportable incidents, metrics for measuring incident response capability, and resources and management supports needed for effectiveness.

The incident response plan will be distributed to all personnel and departments involved with the incident response procedures and will be reviewed, recorded, and documented annually at a minimum, or until significant changes to the college information systems or environments are made, including details of any such changes.

**IR-9: Information Spillage Response**

The CISO will work jointly with the college incident response team to conduct required or necessary incident response procedures and reporting when protected or classified media assets become threatened or vulnerable as described in the Pennsylvania College’s Media Protection Policy.

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>.

Revision History:

*05/03/22 – Policy Modified*

Implementation Date: *04/01/22* Control Area: *NIST SP800-53 R5: PM*

Approval: *Daniel Duncan* Review Date: *05/03/22*

Objective:

The program management plan will describe the Pennsylvania College of Technology’s security requirements and its expected outcomes to develop an information security program and will describe the program management controls and controls used or may be used to meet those requirements.

Purpose:

The program management plan will support the Pennsylvania College of Technology’s mission to provide an information security program to ensure the confidentiality, integrity, and availability of its used, stored, and accessed information media assets, systems, and their environments.

Audience:

The CISO (Chief Information Security Officer) will work jointly with the Pennsylvania College of Technology administrative staff and HR (Human Resources) staff 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 may be subject to compliance with this policy.

Policy:

**PM-2: Information Security Program Leadership Role**

A senior information security officer employed by the college will be referred to as CISO and will be assigned the authority and resources necessary to ensure an effective and successful development and implementation of an information security program.

**PM-3: Information Security and Privacy Resources**

The CISO will work jointly with the relevant Pennsylvania College of Technology administrative staff and HR staff to develop an inventory of required and necessary resources including budgets, staffing, assets, and protected media assets, and will appropriately assign those resources with documentation of classification, authorization, usage, and approval.

**PM-4: Plan of Action and Milestones Process**

The process for the creation of a plan of action and milestones for the information security program will be developed, maintained, and implemented by the CISO including details of the risks to current or future college information media and assets, and to college operations.

Review of this process should be conducted every four years at a minimum, or until significant changes to the information security program, college information systems, or their environments are made.

**PM-5: System Inventory**

The CISO will appoint an ISO or other qualified professions to develop and maintain an inventory of all college information systems and information assets will be developed and maintained annually at a minimum or when significant changes are made to the college information systems.

All PII stored and processed by the college will be assessed and marked appropriately annually at a minimum and will be sanitized as described in the Pennsylvania College of Technology Media Protection Police when deemed appropriate as described by the Personally Identifiable Information Policy.

**PM-6: Measure of Performance**

Outcome based performance metrics including baselines and benchmarking of the information security program will be recorded and documented to develop, monitor, and report on the performance of the information security program.

**PM-7: Enterprise Architecture**

The CISO will determine based on risk the use or maintenance of services on the college campus or off campus including services such as AWS (Amazon Web Services), Azur, or Google Cloud.

**PM-8: Critical Infrastructure Plan**

The CISO will work jointly with the Pennsylvania College of Technology Lead System Administrator to develop, implement, and maintain assets and resources critical to the storage and processing of critical assets. Critical college operations will be defined and documented in the information security program and will include protection strategies as described in the college Media Protection Policy.

**PM-9: Risk Management Strategy**

A comprehensive strategy managing risks to the college information assets, media, and operations including, but not limited to, instances involving PII, HIPAA, and FERPA records will be developed, maintained, and implemented. Reviews will be conducted annually at minimum or when significant changes are made to the college information media or assets, or to college operations.

**PM-11: Mission and Business Process Definition**

The ISO will work jointly with other qualified professionals to ensure the continuity and protection of college business operations, assets, and media by use of incident response and readiness methodologies as defined in the Incident Response Policy including the creation, use, and maintenance of backups with approval and documentation for review by the CISO.

**PM-13: Security and Privacy Workforce**

The Pennsylvania College of Technology will employ a Security Awareness Training and Education program as described by the Awareness Training Policy.

**PM-14: Testing, Training, and Monitoring**

The CISO will ensure the development, implementation, and use of the Awareness Training Policy including assessment, monitoring, and review of the effectiveness of the training and make changes when necessary as described by the Awareness Training Policy.

**PM-15: Security and Privacy Groups and Associations**

The CISO will provide ongoing security awareness and privacy education to faculty, staff, and departments employed by the Pennsylvania College of Technology with access to its’ information system including webinars, conferences, etc. and will associate other college’s including Lock Haven University, Lycoming College, etc. and other security groups on the topics of potential risks and threats to the college.

**PM-17: Protecting Controlled Unclassified Information on External Systems**

The CISO will work jointly with the Pennsylvania College of Technology network administrators to determine the use, storage, and access of controlled media assets to ensure privacy and proper authorization as described by the Media Protection Policy.

**PM-18: Privacy Program Plan**

The CISO will work jointly with the Pennsylvania College of Technology Administration to develop a plan of action to appropriately the handling of confidential or protected information including FERPA, HIPAA, etc. as described by the Personally Identifiable Information Policy.

The Pennsylvania College of Technology Administration will assign an administrative position to oversee the privacy program plan and ensure compliance with federal, local, and state laws and regulations regarding instances of all relevant violations.

**PM-23: Data Governance Body**

The CISO will review, and update policies as described by the individual policies as published and will review documentation regarding retention and classification of data to ensure appropriate use, storage, and access of data.

**PM-26: Complaint Management**

The CISO will work jointly with the Pennsylvania College of Technology administration HR department to develop, implement, and maintain a process for receiving and managing complain, concerns, or questions from individuals about college security and privacy practices.

**PM-28: Risk Framing**

The CISO will work jointly with the ISO, ITS (Information Technology Staff), or other qualified professionals to define, describe, and review risk and vulnerability to the Pennsylvania College of Technology information systems, assets, protected media assets, and their environments as described by the Risk Analysis Policy.

**PM-31: Continuous Monitoring Strategy**

The CISO will appoint the ISO, ITS, or other qualified professional staff to regularly monitor the security of the Pennsylvania College of Technology information systems including system updating, media storage assessment, and closed-circuit security cameras, etc. with documentation recorded and approved by the CISO including details of affected media, changes or updates, dates, and individuals or departments involved.

**PM-32: Purposing**

The CISO will work jointly with the ISO, ITS, or other qualified professional staff to assess and review the Pennsylvania College of Technology information systems, media assets, and their environments to ensure use is consistent with intended purposes as described by the Risk Analysis Policy.

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>.

Revision History:

*05/03/22 – Policy Modified*

Implementation Date: *04/08/22* Control Area: NIST 800-53 R5: AU

Approval: *Daniel Duncan* Review Date: *04/08/22*

Objective:

ITS (Information Technology Staff) and automated information systems will observe traffic and access of the Pennsylvania College of Technology information networks and systems with support from procedures and guidelines of the creation of records and logs including their content, handling of audited assets, and consideration for failure in auditing.

Purpose:

Setting requirements for auditing procedures, guidelines, and necessary tracking, monitoring, and logging of activity on the college information networks and systems will ensure consistency and use of best practices to improve the security of the college information systems.

Audience:

The CISO (Chief Information Security Officer) will work jointly with other qualified professionals such as the ISO (Information Security Officer), ITS, 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:

**AU-2: Event Logging**

The CISO will work jointly with other qualified professionals such as the ISO, ITS, or Third-Party Vendors to develop, maintain, and implement an inventory of definitions of auditable events that could raise suspicion of an attack, threat, or unauthorized use to the Pennsylvania College of Technology information networks or systems including, but not limited to,

* unauthorized user account management or access,
* system or applications errors,
* file creation, deletion, modification, or fail close/open,
* failed and successful account logins,
* changes to administrative privileges,
* and any changes or modifications to logs.

The CISO will distribute this inventory to individuals and departments responsible for event logging, auditing, or reporting auditable events and will review this inventory and make any necessary modifications annually at minimum including details of changes, rationale for changes, date of review and implementation, and systems effected.

**AU-3: Content of Audit Records**

The CISO will assign responsibility to a qualified professional such as the CISO, ISO, ITS, or Third-Party Vendor to develop, maintain, and implement the creation of audit records when an instance of a reportable event occurs as described by the inventory of auditable events definitions.

These records will include, but not limited to, details of event type, date(s) of occurrence, information system effected, location of system, source of event, outcome of event, and individuals involved. Records will be stored with all associated log files of the effected information system(s).

**AU-4: Audit Log Storage Capacity**

The CISO will allocate enough storage, virtual space, and processing power of systems to collect and maintain at a minimum of four years, audit records for review and assessment.

**AU-5: Response to Audit Logging Process Failures**

If audit logging or event capturing failures occur such as failures in information systems software or hardware necessary to record logs, or storage capacity is exceeded, the CISO will be informed, and appropriate actions will be taken to prevent overwriting of records or failure to create new records.

The CISO will work jointly with the ISO and ITS to develop, maintain, and implement procedures to handle audit logging process failures including required steps for protection of stored logs, restoration processes of lost or damaged logs, corrections to effected systems, and will include mechanisms to alert the CISO and other responsible individuals or departments when failures occur or when storage capacity of logs near maximum beginning at 75% and again in increments of 5%.

**AU-6: Audit Record Review, Analysis, and Reporting**

The CISO will work jointly with the ISO and implemented automated monitoring systems to detect and terminate unauthorized activities on the college information networks and systems by monitoring and recording logs to ensure continued operation, security, and privacy of critical or protected assets.

The CISO will appoint a qualified professional such as the CISO, ISO, ITS, or Third-Party Vendor to review audit logs weekly at minimum to detect suspicious or abnormal activities and report these instances to the CISO.

The CISO will work jointly with the ISO and ITS to develop, maintain, and implement procedures to handle threats or attacks to the college information networks and systems including audit logging process failures procedures and will include details of corrective measures to handle instances of unauthorized access.

**AU-8: Time Stamps**

Automated system reporting of audit logs will use an internal system clock generating records of dates and times using EST -5 (Eastern Standard Time) applied to all recorded audit logs.

**AU-9: Protection of Audit Information**

Information and details of audit logs and tools will only be accessible to the CISO, and individuals or departments appointed by the CISO.

Individuals or departments with access to information and details of audit logs and tools will use implemented procedures to protect this information including, but not limited to,

* Backing up audit records on physically different systems or components than effected audited system,
* Recording audit files to log for use before transferring to separate secured location or information system,
* Using encryption of audits while in storage and transit.

**AU-10: Non-Repudiation**

The use or access of college information networks or systems will require proof of identification or will refuse service if authorization cannot be provided using an automated non-repudiation system. Services allowed or refused by this system include, but not limited, access or use of

* protected or private documents,
* sending or receiving messages
* signing contracts
* approving distribution or disclosure of unauthorized information
* etc.

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>

Revision History:

*04/08/22 – Policy Created and Implemented*

Implementation Date: *04/15/22* Control Area: NIST-800 53 R5: CP

Approval: *Daniel Duncan* Review Date: *04/15/22*

Objective:

Contingency Planning will be developed, implemented, and maintained and will include training and education, testing of the Pennsylvania College of Technology information systems, and setting procedures and guidelines of the requirements and expectations of these contingency plans.

Purpose:

The development, implementation, and maintenance of the processes for developing the college contingency plans for the Pennsylvania College of Technology information systems will improve the college’s security and privacy of its’ 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:

**CP-2: Contingency Plan**

The CISO will work jointly with the ISO, the ITS, or a third-party vendor to develop a contingency plan that identifies potential risks and vulnerabilities to college information systems including a plan of action to handle those risks and vulnerabilities.

The contingency plan will include guidelines and procedures for handling downtime of systems from

* downtime as a result of an attack,
* loss, theft, or damage to information,
* natural disasters,
* etc.

The contingency plan will outline the purpose of the plan, expectations of timeline, roles and responsibilities of actors involved, and an effective task layout for completion.

The CISO will review and update contingency plans when significant changes are made to the college information system, environments, operations or at a period of four years at minimum and will appropriately and timely distribute these plans to authorized and relevant personnel.

**CP-3: Contingency Training**

The CISO will work jointly other qualified and professional personnel such as the ISO to provide incident response training and education based on their determined roles and responsibilities.

This incident response training and education will be conducted before assignment of an individual into a role and will include their responsibilities as described by the respective contingency plan and additional training will be provided when significant changes are made to the college information system, environments, operations or annually at a minimum.

Documentation of training will be recorded and maintained for a period of ten years at minimum, including details of administrator of training, date and time, role and responsibilities of trainee, and relevant contingency plans involved.

**CP-4: Contingency Plan Testing**

The CISO will work jointly with other qualified and professional personnel such as the ISO to perform testing on contingency plans developed to handle potential risks and vulnerabilities as described in CP-2 to determine effectiveness and readiness of contingency plans towards the continued security and operation of the college information systems.

Testing will be conducted when significant changes are made to the college information system, environments, operations, contingency plans, or annually at a minimum. Documentation of tests will be recorded for update and review by the CISO for benchmarking and baselining of test results, and continued improvement of contingency planning.

**CP-9: System Backup**

The CISO will ensure a qualified and professional personnel such as the CISO, ISO, or ITS will perform system backups of the college information systems, system assets, and other operation critical college systems such as system files, software, and servers.

Backups will be created when significant changes are made to the college information system, components, environments, operations, or weekly at minimum. Backups will be stored off-site in secure location separate from risks and vulnerabilities that may affect on-site college information systems.

**CP-10: System Recovery and Reconstitution**

The CISO will work jointly with individuals with relevant roles and responsibilities to recover and reconstitute mission critical functionality, processes, and services after disruptions or failures to the college information systems. Documentation of system recovery and reconstitution processes will be recorded to ensure continued effectiveness and correct deployment of contingency plans.

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>

Revision History:

*04/15/22 – Policy Created and Implemented*

Implementation Date: *05/02/22* Control Area: *NIST SP800-218: SSDF*

Approval: *Daniel Duncan* Review Date: *05/02/22*

Objective:

A secure software development plan will be developed, implemented, and maintained to define software security and secure software development best practices to be implemented into the Pennsylvania College of Technology software SDLC (System Development Life Cycle).

Purpose:

The secure software development plan will set requirements and expectations for the guidelines and best practices of secure software development by the college software development team to reduce total number of vulnerabilities, reduce the potential impact of undetected and known vulnerabilities, and prevent future instances of vulnerabilities in software published by the college.

Audience:

The CISO (Chief Information Security Officer) will work jointly with the college Software Development Team and 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:

**SSD-1: Secure Software Awareness**

The CISO will work jointly with the college Software Development Team to identify and document all security requirements for software developed and published by the Pennsylvania College of Technology.

The identified and documented security requirements of software development will include, but not limited to details of:

* Infrastructures and their components including development endpoints,
* Processes including open source or other third-party components,
* Design requirements, including but not limited to, modular code to facilitate reuse and updates, component isolation, and code documentation requirements,
* End of Life or impending End of Life for software support including date and affected systems, notification to appropriate and authorized affected entities, and plan of action
* Necessary information of software release to be recorded including code, package files, libraries, documentation, etc. with details of retention length of this information based on factors such as End of Life,
* Acquisition documentation of software including contracts, and other agreements with third parties
* Other information regarding third-party software usage such as vulnerability disclosure programs, incident response capabilities, compliance with the Pennsylvania College of Technology requirements, etc.

The CISO will review and update security requirements annually at minimum or when significant changes are made to the software development infrastructures or processes and will disclose changes made to security requirements to appropriate and authorized affected entities

**SSD-2: Software Protection**

The CISO will work jointly with the college Software Development Team to develop, maintain, and implement mechanisms to prevent unauthorized access and tampering of all software developed and published by the Pennsylvania College of Technology including, but not limited to:

* Storing of source code, executable code, and CAC (Configuration as Code) in a repository with access restricted to the CISO, the ISO, and members of the Software Development Team based on purpose and impact-level of the code as described by the Pennsylvania College of Technology Risk Analysis Policy,
* Use of version control for accountability of individuals’ modification of code with signatures for committed changes, and review and approval for commits by the code owner
* Use of cryptography to protect code and CA (Certificate Authority) for confirmation of validity before use by users,
* Securely store and maintain software as described by the Pennsylvania College of Technology Media Protection Policy including keeping backups in separate and secure locations,

The CISO will review and update software protection mechanisms annually at minimum or when significant changes are made to the software development infrastructures, processes, assets, components, or environments and will disclose changes made to security requirements to appropriate and authorized affected entities

**SSD-3: Secure Software Production**

The CISO will work jointly with the college Software Development Team to evaluate potential risks to software during operation and develop, implement, and maintain a risk mitigation plan with consideration of software design and architecture.

Role based training will be provided to the Software Development Team members as described by the Pennsylvania College of Technology Awareness Training Policy including assessments of performance in high-risk areas as described by the Pennsylvania College of Technology Risk Analysis Policy.

When appropriate or necessary, as described by the colleges’ Audit and Accountability, Security Assessment and Authorization, and Incident Response policies, the use of standardized security features and services will be integrated into existing software such as log management, identity management, access control, and vulnerability management systems instead of development of software or systems by the college Software Development Team.

Existing software that meets with security requirements described in SSD-1 will be reused when appropriate to reduce additional vulnerabilities and reduce costs of software development. These existing software may include libraries, modules, frameworks, etc. from third-party commercial or open-source development.

Assessment and testing of software will be performed jointly by a senior information security officer and a college Software Development Team member to identify vulnerability and interoperability with relevant existing software or systems. Records of assessment and testing will be documented including details of scope, entities and systems involved, results, discovered issues, recommended remediations, date, approval, and affected software or systems.

Records of security requirements, risks, and design decisions will be documented including details of risk response, mitigation planning and implementation, and exceptions with details of administrator approval, date, affected entities, asset, or software, and rationale behind decisions.

**SSD-4: Vulnerability Response**

Vulnerability Response will help to ensure that vulnerabilities are identified and remediated timely and appropriately as described by the Pennsylvania College of Technology Incident Response Policy and will include information gathering of software used by the college of potential vulnerabilities and components and analysis of this information to address identified vulnerabilities for appropriate response and prevention.

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>

[*https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf*](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf)

Revision History:

*05/02/22 – Policy Created and Implemented*

**CA (Certificate Authority):**

- In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates.

**CAC (Configuration as Code):**

- Configuration as code is the formal migration of config between environments, backed by a version control system.

**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.

**Development Endpoints:**

- An environment that is used to develop and test

**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.

**System Development Life Cycle:**

- The planning, analysis, design, development, implementation, integration and testing, and operations and maintenance of systems.

**AT Control Exclusions:**

**AT-2**:

**AT-3**:

I did not include AT-2, AT-3. In this policy I described the responsibility of determining the scope of the training program to the CISO and did not feel that it was necessary to go into too much detail about the material that must be covered to prevent too many restrictions within that program.

**RA Control Exclusions:**

**RA-4:** NIST SP800-53 R5 now includes this with RA-3

**RA-6:** This was partially included in RA-5, at most I’d include CCTV as a method to do this but I’m not entirely sure how to manage this control as a part of this policy.

**RA-9:** RA-2 assigns responsibility of assigning component definition and category and impact-level. I did not want to be redundant.

**RA-10:** I do not feel that the college would have an employee scale large enough to use active threat hunting, passive threat detection with active response felt more appropriate.

**AC Control Exclusions:**

**AC-3: Access Enforcement**

Not Included. (Wrapped into AC-2)

**AC-5: Separation of Duties**

Not Included. (The college does not have the appropriate resources to implement this control)

**AC-6: Least Privilege**

Not Included. (Wrapped into AC-2)

**AC-8: System Use Notification**

Not Included. (Not necessarily required for implementation on the college systems, may already be addressed in other policies and partial discussion on responsibility assignment in AC-2)

**AC-9: Previous Logon Notification**

Not Included. (Not necessary, other policies and control cover the risk/need of this control)

**AC-10: Concurrent Session Control**

Not Included. (Wrapped into AC-2)

**AC-12: Session Termination**

Not Included. (Wrapped into AC-11)

**AC-14: Permitted Actions Without Identification or Authentication**

Not Included. (Not necessary for the college systems)

**AC-16: Security and Privacy Attributes**

Not Included. (Wrapped into AC-4)

**AC-17: Remote Access**

Not Included. (Wrapped into AC-4)

**AC-18: Wireless Access**

Not Included. (Wrapped into AC-4)

**AC-19: Access Control for Mobile Devices**

Not Included. (Wrapped into AC-4)

**AC-20: Use of External Systems**

Not Included. (The college does not have the appropriate resources to implement this control/Is not necessary to fulfill college mission)

**AC-21: Information Sharing**

Not Included. (Wrapped into AC-4)

**AC-23: Data Mining Protection**

Not Included. (The college does not have the appropriate resources to implement this control)

**AC-24: Access Control Decisions**

Not Included. (The college does not have the appropriate resources to implement this control/Partially wrapped into AC-2)

**AC-25: Reference Monitor**

Not Included. (The college does not have the appropriate resources to implement this control/Partially wrapped into AC-2)

**PT Control Exclusions:**

**PT-4: Consent**

Not Included. (Wrapped into PT-1)

**PT-6: System of Records Notice**

Not Included. (This control does not apply to the college)

**PM Control Exclusions:**

**PM-10: Authorization Process**

Not Included. (Implied in normal business environments, included with the authorization/approval given by the CISO in the inventory/resource list and designation/assignment of those resources in PM-3)

**PM-12: Insider Threat Program**

Not Included. (This should already be addressed in Risk Analysis. Resources responsible for addressing risk should already take insider threats into account. A program specific to insider threats may require resources unavailable to an organization of our size.)

**PM-16: Threat Awareness Program**

Not Included. (PCT may not be large enough to dedicate resources to this.)

**PM-19: Privacy Program Leadership Role**

Not Included. (Wrapped into PM-18)

**PM-20: Dissemination of Privacy Information**

Not Included. (Wrapped into PM-18)

**PM-21: Accounting of Disclosure**

Not Included. (Wrapped into PM-18)

**PM-22: Personally Identifiable Information Quality Management**

Not Included. (Wrapped into PM-18)

**PM-25: Minimization of Personally Identifiable Information Used in Testing, Training, and Research**

Not Included. (Wrapped into PT-3)

**PM-27: Privacy Reporting**

Not Included. (Wrapped into PM-18)

**PM-29: Risk Management Program Leadership Roles**

Not Included. (Wrapped into PM-28)

**PM-30: Supply Chain Risk Management Strategy**

Not Included. (The college does not have enough control over its supply chain to need a control for it.)

**AU Control Exclusions:**

**AU-7: Audit Records Reduction and Report Generation**

Not Included. (Controls included present enough support/information to cover what this control would provide. I.E AU-3, 5, 6)

**AU-11: Audit Record Retention**

Not Included. (Wrapped into AU-4, 6)

**AU-12: Audit Record Generation**

Not Included. (Wrapped into AU-2, 3)

**AU-13: Monitoring for Information Disclosure**

Not Included. (Wrapped partly into AU-2, college resources likely are not extensive enough to cover monitoring outside sources for this specifically, AT, MP, IR, RA, and PM have descriptions that support the protection and response to disclosure of PII and other protected information assets)

**AU-14: Session Audit**

Not Included. (College resources may not be able to handle session auditing, instances of suspicious or abnormal activity or behaviors on the college networks or systems should be included in AU-2 and AU-6 and handling of these activities are supported by AU-6 and AU-10)

**AU-16: Cross-Organizational Audit Logging**

Not Included. (College resources may not be able to handle cross-organizational audit logging and may pose a risk not necessary for college operations and security.)

**CP Control Exclusions:**

**CP-6:**

Wrapped into CP-9

**CP-7:**

The college does not have the appropriate resources to implement this control

**CP-8:**

The college does not have the appropriate resources to implement this control

**CP-11:**

Wrapped into CP-10

**CP-12:**

The college does not have the appropriate resources to implement this control

**CP-13:**

The college does not have the appropriate resources to implement this control