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)

Definitions:

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.

Revision History:

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