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

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>

Definitions:

CISO (Chief Information Security Officer):

* The senior most level executive security professional within the organization of the Pennsylvania College of Technology responsible for the protection of the College’s information assets and programs.

Control:

- The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.

Incident:

- An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Assets:

* A body of information defined and managed as a single entity within the organization which may have financial value.

Information System:

* A system organized to collect, process, store, and distribute information including but not limited to computer systems, people, documents, and technology.

ISO (Information Security Officer):

* A security professional within the organization of the Pennsylvania College of Technology responsible for assisting the CISO with the protection of the College’s information assets and programs.

PII (Personal Identifiable Information)

* Any representation of information that allows for the identification of to whom the information applies to be reasonably inferred by either directly or indirectly.

Policy:

* A statement of intent provided to establish procedures and guidelines to direct decisions and actions of the College.

Risk

- The potential for loss or damage when a threat exploits a vulnerability.

Revision History:

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