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

Approval: *Daniel Duncan* Review Date: *03/25/22*

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) Staff, 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 procedures. 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.

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:

*03/25/22 – Policy Created and Implemented.*