Implementation Date: *04/08/22* Control Area: NIST 800-53 R5: Audit & Accountability

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>

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:

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