Pennsylvania College of Technology

Policy Statement

Title: Information Security

Number: P 8.02

Approved by:
Presidential Action

Approved Date: 11/01/2022
Implementation Date: 11/2022
Last Review Date: 11/2022
Last Revision Date: 11/2022

Persons/Departments Affected:
All employees and students

Responsible Department:
Information Technology Services

Policy:

I. INTRODUCTION

The purpose of this policy is to assist the institution in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets and comply with regulatory and contractual requirements involving information security and privacy. This policy framework consists of eighteen (18) separate policy statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53 r4.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive privacy structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity, and availability of the institution's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

II. PURPOSE

The purpose of this Information Security Policy is to clearly establish Pennsylvania College of Technology's (Penn College's) role in protecting its information assets and communicating minimum expectations for meeting these requirements. Fulfilling these objectives enables Penn College to implement a comprehensive system-wide Information Security Program.

III. SCOPE

The scope of this policy includes all information assets governed by the institution. All students, faculty, staff, students, student workers and service providers who have access to or utilize assets of the institution, including data at

rest, in transit or in process shall be subject to these requirements. This policy applies to:

a. All information assets and information technology (IT) resources operated by the institution.

b. All information assets and IT resources provided by the institution through contracts, subject to the provisions and restrictions of the contracts; and

c. All authenticated users of Penn College information assets and IT resources.

IV. IMPLEMENTATION

Penn College needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill the institution's mission. The Information Security Program must be risk-based, and implementation decisions must be made based on addressing the highest risk first.

Penn College's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to institution limitations and resource constraints. Administration must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

V. ROLES AND RESPONSIBILITIES

Penn College has assigned the following roles and responsibilities:

a. Vice President for Information Technology and Chief Information Officer: The VP IT/CIO is accountable for the implementation of the Information Security Program including Security policies, standards, and procedures. Security compliance including managerial, administrative, and technical controls. The VP IT/CIO is to be informed of information security implementations and ongoing development of the Information Security Program design.

b. Information Security Committee: The group is responsible for the design, implementation, operations, and compliance functions of the Information Security Program for all Penn College constituent units. The committee is comprised of President's Council or designees.

c. Director of Information Security & Privacy: This position is responsible for the development, implementation, and maintenance of a comprehensive Information Security Program for Penn College. This includes security policies, standards and procedures which reflect best practices in information security.

VI. INFORMATION AND SYSTEM CLASSIFICATION

Penn College must establish and maintain security categories for both information and information systems. For more information, reference the P8.04 Data Classification.

VII. PROVISIONS FOR INFORMATION SECURITY STANDARDS

The Penn College Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on SANS Critical Security Controls priorities. Penn College must develop appropriate control standards and procedures required to support the institution's Information Security Policy. This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification.

The Penn College Information Security Program is based on NIST Special Publication 800-53. This publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements.

a. ACCESS CONTROL (AC)

Penn College must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

b. AWARENESS AND TRAINING (AT)

Penn College must:

i. ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of institution information systems
ii. ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities

All College employees handling confidential or private information shall be required to complete an information security professional development within 6 months of their hire date. Continuing education will be required at a frequency determined by Information Technology Services and The Office of People & Culture.

c. AUDIT AND ACCOUNTABILITY (AU)

Penn College must:

i. create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum

ii. ensure that the actions of individual information system users can be uniquely traced for all restricted systems

d. ASSESSMENT AND AUTHORIZATION (CA)

Penn College must:

i. periodically assess the security controls in institution information systems to determine if the controls are effective in their application
ii. develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in institution information systems
iii. authorize the operation of the institution's information systems and any associated information system connections
iv. monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls

e. CONFIGURATION MANAGEMENT (CM)

Penn College must:

i. establish and maintain baseline configurations and inventories of institution information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles
ii. establish and enforce security configuration settings for information technology products employed in institution information systems

f. CONTINGENCY PLANNING (CP)

Penn College must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the institution's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

g. IDENTIFICATION AND AUTHENTICATION (IA)

Penn College must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Penn College information systems.

h. INCIDENT RESPONSE (IR)

Penn College must:

i. establish an operational incident handling capability for institution information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities
ii. track, document, and report incidents to appropriate institution officials and/or authorities

i. MAINTENANCE (MA)

Penn College must:

i. perform periodic and timely maintenance on institution information systems
ii. provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance

j. MEDIA PROTECTION (MP)

Penn College must:

i. protect information system media, both paper and digital
ii. limit access to information on information system media to authorized users
iii. encrypt, where applicable
iv. sanitize or destroy information system media before disposal or release for reuse

k. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Penn College must:

i. limit physical access to information systems, equipment, and the respective operating environments to authorized individuals
ii. protect the physical plant and support infrastructure for information systems
iii. provide supporting utilities for information systems
iv. protect information systems against environmental hazards; and
v. provide appropriate environmental controls in facilities containing information systems.

l. PLANNING (PL)

Penn College must develop, document, periodically update and implement security plans for institution information systems that describe the security controls in place or planned for the information systems as well as rules of behavior for individuals accessing the information systems.

m. PERSONNEL SECURITY (PS)

Penn College must:

i. ensure that individuals occupying positions of responsibility within the institution are trustworthy and meet established security criteria for those positions
ii. ensure that institution information and information systems are protected during and after personnel actions such as terminations and transfers
iii. employ formal sanctions for personnel failing to comply with Penn College security policies and procedures.

n. RISK ASSESSMENT (RA)

Penn College must periodically assess the risk to institution operations (including mission, functions, image, or reputation), institution assets, and individuals,

resulting from the operation of institution information systems and the associated processing, storage, or transmission of institution information.

o. SYSTEM AND SERVICES ACQUISITION (SA)
Penn College must:

i. allocate sufficient resources to adequately protect institution information systems
ii. employ system development life cycle processes that incorporate information security considerations
iii. employ software usage and installation restrictions; and
iv. ensure that third- party providers employ adequate security measures, through federal and state law and contract, to protect information, applications and/or services outsourced from the institution

p. SYSTEM AND COMMUNICATIONS PROTECTION (SC)
Penn College must:

i. monitor, control and protect institution communications (i.e., information transmitted or received by institution information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions
ii. ii. employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within institution information systems

q. SYSTEM AND INFORMATION INTEGRITY (SI)
Penn College must:

i. identify, report and correct information and information system flaws in a timely manner
ii. provide protection from malicious code at appropriate locations within institution information systems
iii. monitor information system security alerts and advisories and take appropriate actions in response

r. PROGRAM MANAGEMENT (PM)
Penn College must implement security program management controls to provide a foundation for the institution's Information Security Program.

VIII. ENFORCEMENT

Penn College may temporarily suspend or block access to any individual or device when it appears necessary to do so to protect the integrity, security, or functionality of institutional and computer resources.

Any personnel found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment or enrollment.

IX. PRIVACY

Penn College must make every reasonable effort to respect a user's privacy. However, personnel do not acquire a right of privacy for communications transmitted or stored on institution resources.

Additionally, in response to a judicial order or any other action required by law or permitted by official institution policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the Vice President for Information Technology and Chief Information Officer (VP IT/CIO), or an authorized agent, may access, review, monitor and/or disclose computer files associated with an individual's account.

X. EXCEPTIONS

Exceptions to the policy may be granted by the Vice President for Information Technology and Chief Information Officer (VP IT/CIO) or their designee. To request an exception, submit an Information Security Exception request to the Director of Information Security and Privacy.

XI. DISCLAIMER

Penn College disclaims any responsibility for and does not warrant information and materials residing on non-Penn College systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of Penn College.

XII. REFERENCES

- NIST SP 800-53
- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Pennsylvania's Breach of Personal Information Notification Act
- FIPS-199
- PCI DSS 4.0

Revision History:

Date:
Date:
Date:

Cross References:

- Data Classification Policy P8.04
- Acceptable Use Policy P8.03
- Family Educational Rights/Privacy Act P4.04