Pennsylvania College of Technology

Policy Statement

Title: Written Information Security Program

Number: P 8.01

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 objectives of this Written Information Security Program (WISP) are to define, document and support the implementation and maintenance of the administrative, technical, and physical safeguards Pennsylvania College of Technology (PCT) has selected to protect the information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the following security best practices and regulations:

a. NIST Special Publication 800-53 – The NIST Special Publication 800-53 standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls, customized to the needs of individual organizations, or parts thereof.

b. Payment Card Industry Data Security Standards (PCI DSS) v4.0 - Contractual obligations addressing the administrative, technical, and physical standards required by payment brands (Visa, AMEX, MasterCard, Discover) for organizations processing payment card transactions.

c. Gramm-Leach-Bliley Act (GLB Act or GLBA) - Federal law enacted in 1999 which requires organizations that loan money to take measures to protect the financial information of individuals.

d. Family Educational Rights and Privacy Act (FERPA) - Federal law enacted in 1974 requiring any school receiving federal funds to protect the privacy of educational records.

e. General Data Protection Regulation (GDPR) - The General Data Protection Regulation is a European Union law that was implemented on May 25, 2018 and requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. The regulation includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines.

f. California Consumer Privacy Act (CCPA) - The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States. The bill was passed by the California State Legislature and signed into law by Jerry Brown, Governor of California, on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code.

g. Health Insurance Portability and Accountability Act (HIPAA) – Enacted by the U.S. Congress in 1996 that mandates covered entities to implement reasonable and appropriate security measures to protect all electronic protected health information (ePHI) against reasonably anticipated threats or hazards.

h. Massachusetts 201 CMR 17.00 – Massachusetts regulation that establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.

    a. This document is intended to satisfy Massachusetts Data Security Regulation 201 C.M.R 17 requirement for a WISP and NIST standards for maintaining a Critical Infrastructure Plan (CIP).

II. VISION, MISSION, AND GOALS

a. Vision
A robust NIST-based security program supported by policies, standards and procedures that address the eighteen (18) NIST security domains.

b. Mission
Strengthen the security of PCT's environment by implementing a structured security program and ensuring that the relationship between information security and the business objectives of PCT exists and is effective.

c. Goals
Deploy security controls to reduce risk for information assets, as defined by specific goals. Achieving these goals requires that PCT:

i. Align information security initiatives with business strategy.
ii. Assign ownership and accountability for information security initiatives.
iii. Monitor the status and efficacy of information security initiatives.
iv. Institute a process of continuous assessment and improvement.

III. CORE TENANTS

PCT's WISP establishes five core tenants, representing the values and assumptions that will be considered when implementing the information security program.

a. Risks are identified and managed in a coordinated and comprehensive way across PCT environment to enable effective allocation of information security resources. This involves promoting efficient and effective use of resources by taking a comprehensive and strategic approach to risk management.

b. Understanding and accounting for dependencies within PCT’s environment when managing risks is critical to enhancing information security.
c. Information sharing amongst PCT’s environment is paramount to gaining knowledge of information security risks.
d. Partnership in implementing PCT’s information security program allows for unique perspectives in understanding information security gaps, challenges, and solutions.
e. Information security will be factored into all decisions regarding PCT assets, systems, and networks.

IV. ROLES AND RESPONSIBILITIES:

Information Security Leadership

To successfully manage risk across PCT, senior leaders and executives must be committed to making information security a fundamental mission. This top-level, executive commitment ensures that sufficient resources are available to develop and implement an effective, organization-wide security program. Effectively managing information security risk organization-wide requires the following key elements:

a. Assignment of risk management responsibilities to senior leaders and executives.
b. Ongoing recognition and understanding by senior leaders and executives of the information security risks to organizational information assets, operations, and personnel.
c. Establishment of the tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities; and
d. Providing accountability for senior leaders and executives for their risk management decisions.

Information Security Officer

The Director of Information Security and Privacy will be appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. Responsibilities will include:

a. Development, maintenance, and distribution of policies and procedures
b. Ensuring responsibilities and assignment for monitoring alerts
c. Incident response processes are understood and performed
d. Development, maintenance, and implementation of a security incident response plan.
e. Ensure access control processes are defined and implemented
f. Ensure all access control processes are monitored

Information Security Steering Committee

The Information Security Steering Committee facilitates active participation of business leaders in information security decision-making. The Information Security Steering Committee often participates in the following:

a. Establishing goals for the Information Security program.
b. Reviewing and approving Information Security policies and standards.
c. Recommending, reviewing, and prioritizing information security initiatives.
d. Communicating information security needs.
e. Reviewing the effectiveness of the information security program and resources.
f. Ensuring corrective action plans have been developed and implemented to address risks that are unacceptable to PCT.

The WISP will establish the Information Security Steering Committee and ensure its ongoing operation.

V. RESOURCE OPTIMIZATION

PCT dedicates resources to information security initiatives to reduce risk, and subsequently meet business objectives. It is understood that these resources are finite and specific, and of the following types:

a. Budget – Funds for information security initiatives will be allocated on an annual basis. Allocated funds are determined by business needs, which will be determined by organizational risk.
b. Personnel – The information security team consists of both physical and virtual members, full-time employees, partners, and subcontractors. The number of personnel allocated to information security initiatives is determined by business need, which will be determined by organizational risk. These are allocated and leveraged optimally based on capabilities and availability.
c. Time – The information security team is granted time to complete security initiatives. Schedules for security initiatives are determined by business needs, which will be determined by organizational risk.

VI. STRATEGY

a. Overview

The key to ensuring that PCT’s security program is reasonable and useable is to develop a suite of policy documents that match the intended audience’s business goals and culture. Policies must be practical and realistic. To achieve this, it is essential to involve and obtain support from senior management and other stakeholders, as well as from the people who will use the policy as part of their daily work.

The organization will:

i. Develop and disseminate information security program standards and an information security plan that provides an overview of the requirements for the security program, a description of the security program management controls and common controls in place or planned for meeting those requirements.

ii. Establish and maintain organizational policies, standards, and procedures to address all relevant statutory and regulatory requirements, and ensure and support the confidentiality, integrity, and availability of its information assets.

iii. Make relevant policies, standards, and procedures readily available to all effected workers.

iv. Conduct a periodic formal review of policies, standards, and procedures and update them, at a minimum, annually.

b. Policy Implementation

The PCT Information Security Program is based on the following foundational Security Policies:

i. Acceptable Use Policy – Advises all members of PCT on acceptable and unacceptable behavior involving the organization's resources.

ii. Data Classification Policy – Describes the process for classification and handling of the organization's data.

iii. Information Security Policy – Creates provisional compliance requirements for the PCT Information Security Standards. Requires that all PCT administrative and business functions meet minimum requirements for security.

iv. Public and Employee Privacy Policies - Advises and informs all constituents of PCT's privacy practices. Including the specification of objectives, rules, obligations, and privacy controls with regard to the processing of personal information and the subjects' rights in regard to the data that is collected.

c. Standards Implementation

PCT has developed appropriate control standards, herein referred to as Information Security Standards, to support the Organization's Information Security policies. These standards are based on NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations". The Information Security Standards define all PCT directives for safeguarding information and ensuring that each organization complies with applicable laws, regulations, and commercial standards. Appropriate procedures have been documented that describe the tools, processes, and resources used to implement the Information Security Standards. The PCT Information Security Standards are structured into eighteen (18) control groups.

Wherever appropriate, information security controls will comply with, reference, and implement the above standards.

d. Regulatory and Security Best Practice Compliance

While not currently mapped to PCT Information Security Standards, PCT must also comply with the following:

i. Electronic Communications Privacy Act (ECPA) - Federal law which specifies the standards by which law enforcement is permitted to access to electronic communications and associated data, affording important privacy protections to subscribers of emerging wireless and Internet technologies.

ii. U.S. Patriot Act - An antiterrorism law enacted by the U.S. Congress in October 2001, which gave certain additional new powers to the U.S. Department of Justice, the National Security Agency and other federal agencies for surveillance of electronic communications.

iii. Technology Education and Copyright Harmonization Act (TEACH) - Amendments to sections 110(2) and 112(f) of the U.S. Copyright Act., which was enacted to balance the perspectives of both copyright owners and content users for academic organizations.

iv. Executive Order 13224 - Federal Executive Order which provides a means to disrupt the financial support network for terrorists and terrorist organizations by authorizing the U.S. Government to designate and block the assets of foreign individuals.

v. Pennsylvania's Breach of Personal Information Notification Act P.L. 474, No. 94 Cl. 12 - Pennsylvania State Law requiring notification to individuals and State agencies after a security incident has occurred involving the loss or unauthorized access to certain private non-public information.

vi. Higher Education Opportunity Act (HEOA) - Federal law which, among other requirements, addresses colleges and universities responsibilities relating to copyrighted materials.

It is the goal and intent of the WISP to ensure compliance with all known regulations and mandates as they are understood, and to make them an appropriate priority.

VII. RISK MANAGEMENT

a. Set Goals and Objectives
Goals and objectives for PCT's information security program will be established and corrective action plans (CAPs) will be documented and prioritized according to risk to the organization.

b. Identify Infrastructure
PCT will identify all assets, systems, and networks critical to continued operation, as well as the dependencies between these essential resources. Effective risk management requires an understanding of the criticality of these resources to the organization.

c. Assess and Analyze Risks
Identifying risks is the single-most important step an organization can take to ensure the confidentiality, integrity, and availability of information assets. It is also an important component for achieving regulatory, commercial, and legal compliance.

d. The determination of Global Risk Tolerance

Assigning a number between 1 and 25 (where 1 is entirely risk-averse and 25 is entirely risk-tolerant), will be performed through an informal survey of organization executives and stakeholders. The Global Risk Tolerance will be used as a suggested remediation threshold during risk management – any risk that exceeds this level will and should be used to prioritize remediation and define corrective action plans.

e. Risk Reduction
Prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. The organization will implement security measures that reduce the risks to its information systems containing confidential information to reasonable and appropriate levels. Selection and implementation of such security measures will be based on a formal, documented risk management process.

f. Implement Risk Management Activities
The organization will manage risk on a continuous basis and implement necessary security measures to ensure the confidentiality, integrity, and availability of information systems containing confidential information. A risk assessment will be performed at least once per calendar year. This involves identifying the risks to information assets and determining the probability of occurrence, the resulting impact, and additional safeguards to mitigate this impact. Strategies for managing risk should be commensurate with the risks to such systems. One or more of the following methods may be used to manage risk:

i. Risk acceptance – The institution accepts responsibility for the risk and the potential costs and impacts if the risk is realized.
ii. Risk avoidance – The institution avoids the risk by altering plans or activities.
iii. Risk limitation – The institution implements measures to reduce the probability and/or impact of the risk to an acceptable level.
iv. Risk transference – The institution transfers the risk to a third party, such as an insurance carrier or service provider. Note some risks cannot be fully transferred.

The organization will manage the security state of organizational information systems and the environments in which those systems operate through a security authorization processes.

i. The Director of Information Security and Privacy will be responsible for performing a risk assessment ensuring adequate security controls are in place for all new services/capabilities/technologies being implemented prior to being put into a production state.

This position on risk management will be stated and reinforced in the security policy.

g. Measure Effectiveness

PCT will regularly evaluate the progress of security program implementation and risk management by reviewing and updating CAPs. Progress will be communicated to necessary stakeholders.

VIII. COMPUTER AND TECHNOLOGY OPERATIONS

a. General

Computer systems and networks, communications systems and other equipment belonging to or otherwise in the possession of PCT are the property of PCT and will be maintained solely by PCT. These systems are provided for use in conducting PCT business, although reasonable personal use by workforce is permitted. Only PCT owned assets will be used to process, store, or transmit PCT owned data or information. The use of any PCT system for commercial purposes other than that of PCT is prohibited. There is no expectation of privacy when using any PCT computers, systems, networks, or other equipment and PCT reserves the right to obtain access to any and all communications and data or information stored, processed, or transmitted by these systems at any time and without prior notice.

b. Network Security

PCT network will be maintained in such a way that risk of corruption of data and unauthorized internal and external access is minimized. Vulnerabilities that arise in PCT's network will be addressed according to PCT's Vulnerability Management procedure. For more information on network security, reference Policy 8.03\Acceptable Use.

c. Endpoint and Removable Media Protection

Controls will be implemented on PCT laptops and removable media to protect the confidentiality and integrity of information contained therein.

- i. PCT laptops and removable media will be encrypted.
- ii. PCT computing devices will be configured to time out and log out settings.
- iii. End users will protect all PCT owned computing devices and removable media.
- iv. Virus detection and protection solutions will be implemented on PCT-owned computing devices.
- v. PCT workforce will report any issues, including theft, immediately to Information Technology Services.

For more information on endpoint and removable media protection, reference Policy 8.03\Acceptable Use.

d. User ID's and Passwords

All PCT users will be provided with a unique username and password to access any PCT-owned system or application. PCT user's passwords will be required to meet minimum length, complexity, and reuse requirements in an attempt to protect confidential or sensitive data. In addition to a unique username and password, some systems may require Multi-Factor Authentication. In these instances, workforce members will be required to provide additional authenticator information such as a token or other factor to prove identity prior to gaining access to critical systems and data. All work users will protect and not misuse user ID's and passwords.

e. Access Rights

Only approved workforce will have access to PCT systems and information and will be provided with the minimum level of access necessary to complete job duties. Network controls will be applied to prevent unauthorized network access. Any devices logged onto PCT's network will be configured to time out.

Remote access to PCT's environment will be granted only to those users with a legitimate documented business need.

Access to PCT information, regardless of the form of information, will only be performed for legitimate business purposes. No user is permitted to access, read, edit, print, copy, transfer or delete information maintained by any other user unless given permission to do so by the Data Owner. Access to systems owned or operated by PCT's third-party vendors is not permitted without proper authorization.

f. System Monitoring

At the discretion of the President, PCT reserves the right to monitor or review activity on any organization-owned system and without notice. Banners explaining PCT's position on system monitoring will be implemented on all assets where logins happen.

g. Data Classification and Handling

PCT workforce will classify and label all information and data. PCT workforce will make all efforts to redact any information classified as confidential or sensitive when appropriate to do so. PCT data and information will be retained according to applicable local and federal guidelines. All PCT data and information will be destroyed when no longer needed. PCT workforce will be responsible for appropriately processing, storing and transmitting PCT information or data. For more information on data classification and handling, reference Policy 8.04\Data Classification, Policy 7.23\Record Maintenance & Retention, and Policy 4.04\FERPA.

h. Acceptable Use

All users will appropriately use PCT computer systems and networks, communications systems and other equipment belonging to PCT, and in such a way that does not violate any law or regulation. Examples include, but are not limited to:

i. Voicemail
ii. Software
iii. Email
iv. Internet

For more information on acceptable use, reference Policy 8.03\Acceptable Use.

i. Personnel Security

All PCT users will be provided with all relevant and necessary policies, standards, and procedures necessary to perform job duties upon hire and annually. PCT users will be provided with relevant training on these topics and will be expected to attest to having read and understood all materials provided. PCT will assign a risk designation to each position and screen, transfer and terminate workforce appropriately.

j. Vendor Management

PCT enters into contracts with third-party vendors for essential services. PCT will conduct reasonable due diligence on vendors. PCT will ensure all reasonable and appropriate agreements are in place to protect any PCT data or information processed, stored, or transmitted by third-party vendors. Any vendor processing, storing, or transmitting information in scope of FERPA should have a statement in agreement with Policy 4.04\Family Educational Rights/Privacy Act.

IX. EXCEPTIONS

Compliance with the PCT WISP, along with related policies, standards and procedures are necessary to ensure the confidentiality, integrity, and availability of organizational information assets. PCT leadership recognizes, however, that full compliance with the WISP may not be possible, due to operational constraints. Non-compliance with any organization standard will be documented as an exception, reviewed, approved, and addressed. Documented exceptions will include:

a. The standard where non-compliance may exist.
b. The specific non-compliant situation, service, or process.
c. The operational risk introduced by the gap.
d. Any current controls which may partially mitigate the risk.
e. If the decision is to remediate the gap, a corrective action plan (CAP) must be developed and assigned to an owner.
f. The acceptance of the risk and remediation plans.

X. INFORMATION SECURITY ROAD MAP

The Information Security Roadmap describes the current and planned security priorities of the organization.

XI. REFERENCES

Regulation

- http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

Compliance Checklist

- http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf

Revision History:

Date:
Date:
Date:

Cross References:

Acceptable Use Policy P 8.03
Data Classification and Handling Procedure P 8.04
Family Educational Rights and Privacy Act (FERPA) P 4.04
Information Security Policy P 8.02