PRATT
Community College

ADMINISTRATIVE POLICY

Number	600-10
Adoption	01-01-2018
Deletion	
Revision	
Review Date	

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Pratt Community College will develop, implement and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards to protect covered information. Training in collecting, accessing and handling of covered information promoting the awareness and compliancy of the information security program.

This policy outlines the security requirements to ensure compliance with the Gramm-Leach-Bliley Act (GLBA) (Public Law 106-102) and the Federal Student Aid (Title IV) Program Participation Agreement and SAIG agreement. Utilize guidelines from NIST Special Publication 800-171 Revision 1. This policy applies to all Pratt Community College employees and third parties that create, access, store or manage CUI. The following security requirement families are covered by this policy: access control, awareness training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, system and communications protection and system and information integrity.

The objectives of the policy are the following: 1) protect the confidentiality and integrity of personal information, 2) proactive approach to risks that can potentially threaten the security and integrity of protected information, 3) prevent unauthorized access to protected information that would cause harm or inconvenience to the customer.

Covered Information

Information derived by a collection means from a customer, by or on behalf of Pratt Community College, for the offering of financial products or services. Financial products or services are offering student loans to students, receiving income tax information from a student’s parents or legal guardian in an effort to attain a financial aid package, and other miscellaneous financial services. Financial information attained include but are not limited to address, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in verbal, paper or electronic format.

Related Policies

Red Flag Rules – Policy 600-08
Employee Training for Security Awareness – Policy 600-09

Basic Security Requirements

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.

Establish and enforce security configurations settings for information technology products employed in organizational systems.

Derived Security Requirements

Track, review, approve and audit changes to systems.
Analyze the security impact of changes prior to implementation.
Define, document, approve and enforce physical and logical access restrictions associated with changes to systems.

Employ the principle of least functionality by configuring systems to provide only essential capabilities.

Restrict, disable and prevent the use of nonessential programs, functions, ports, protocols and services.

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all-permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Control and monitor user installed software.

Roles and Responsibilities

The Vice-President of Finance and Operations is responsible for the information security program. The program will be reviewed annually to perform a risk assessment and determine necessary changes based on required testing/monitoring, material changes in operations or business arrangements or any other circumstances that have a material impact on the information security program.

The Director of Information Technology is responsible for coordinating and recommending changes to the security program, performing annual risk assessments, coordinating training programs and recommending additional safeguards.

Information Security Program Working Group is responsible for determining issues that need to be addressed and determining changes that are required to the policy. The committee will be comprised of the Director of IT, DB Administrator, Registrar, Controller, Financial Aid Director, Vice-President of Finance and Operations, Data Management Coordinator and Vice-President of Instruction.

Reporting Breaches to the Department of Education

Actual data breaches, as well as suspected data breaches must be reported on the day a data breach is detected or even suspected. Breaches should be reported to email cpssaig@ed.gov. The following information must be included in the email:

Date of the breach (known or suspected).

Impact of the breach (number of records, number of students, etc.).

Method of the breach (hack, accidental, disclosure, etc.).

Information security point of contact (email and telephone number).

Remediation status (complete, in-process, etc.).

Next steps (as needed).

Information Security Program Elements

Risk Assessment

Risk and privacy assessments are used to determine the probability and magnitude of harm to the college's information systems, the affected individual(s), and the legal as well as the reputation of the college itself in the event of a security breach. Determining the amount of risk that exists facilities the college's decision on how much risk should be mitigated and what controls are necessary to achieve that mitigation assessment.

Risk and privacy assessments are performed for all information systems that access or store covered information with guidance from the Vice President of Finance and Operations at least on an annual basis. Elements of the risk and privacy assessments include unauthorized access, use, disclosure, disruption, modification, and/or destructions of information or the information system itself. The identification of known potential threats, the likelihood of their occurrence and their magnitude of impact on Pratt Community College should they occur are included in the risk assessment.

Internal and external risks at Pratt Community College include, but are not limited to:

> Unauthorized access of covered information by persons within or outside the University
>
> Compromised system security as a result of human error, vulnerabilities, infection by malicious software, or unauthorized system access
>
> Interception of data during transmission
>
> Loss of data integrity
>
> Physical loss of data in a disaster
>
> Errors introduced into the system
>
> Corruption of data or systems
>
> Unauthorized access through hardcopy files or reports
>
> Unauthorized disclosure of covered information through third parties

Risk and privacy assessments shall be performed on new information systems acquisitions or changes to current information systems prior to initial establishment of service agreements. Further, the risk and privacy assessment shall be reviewed every three years or whenever a significant change is made to the information system.

Risk assessment should include consideration of risks in each of the following operational areas, in accordance with the requirements of the GLBA:

<u>Employee training and management</u>

New employees in positions that require access to covered information, prior to being granted access to covered information, will receive training on the importance of confidentiality of student records, financial information, health information, and other types of covered information as well as the risks of not providing appropriate protection. All college employees are to receive annual training in the accessing and handling of general information security. Training will include controls and procedures to restrict employee from disclosure of confidential information to an unauthorized individual through social engineering or improper disposal of document that contain covered information. All training will be documented, reviewed and updated as needed annually.

Departments which access or maintain covered information are to take steps to protect information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

For additional training details see administrative policy 600-09.

Information systems

Includes network components and software design as well as information processing, storage, transmission, and disposal.