3.14 Identity Theft Prevention Program

Last Revised: September 2023

Policy: The Board of Trustees of Piedmont Community College (PCC) enacts reasonable procedures to protect students and college employees from damages associated with the compromise of sensitive personally identifiable information.

Purpose/Definitions:

Purpose

The purpose of this policy is to describe procedures to protect students and college employees from damages associated with the compromise of sensitive personal information.

Definitions

Creditor—any organization, including community colleges, which regularly extends, renews, or continues credit; or arranges for someone else to extend, renew, or continue credit; or is the assignee of a creditor involved in the decision to extend, renew, or continue credit.

Credit—deferral of payment of a debt incurred for the purchase of goods or services, including educational services.

Financial institution—typically a bank, credit union, or other entity that holds for an individual an account from which the owner can make payments and transfers.

Identity theft—a fraud attempted or committed using identifying information of another person without proper authority.

Information Technology Services (ITS)—the acronym used to designate Information Technology Services.

Red Flag—a pattern, practice, or specific activity which indicates the possibility of identity theft.

Red Flag Task Force and its recommendations—as a result of the increasing instances of identity theft, the United States Congress passed Public Law 108-159, the Fair and Accurate Credit Transactions Act of 2003 (FACTA). This amendment to the Fair Credit Reporting Act dictated that the Federal Trade Commission (FTC) promulgate rules to address identity theft. The rules promulgated by the FTC (Red Flag rules) require any financial institution or creditor that holds any type of consumer account or other account for which a potential risk of identity

theft exists to create and implement a written Identity Theft Prevention Program to thwart identity theft associated with new and existing accounts.

Sensitive personally identifiable information—information belonging to any student, employee, or other person with whom the College is affiliated that is not open to the public or is not considered directory information. See PCC Policies 5.7.1 Employee Personnel File and 7.6 The Family Educational Rights and Privacy Act of 1974 for more information.

Student records—any records containing information concerning academics and enrollment (curriculum, adult, and continuing education), financial aid, finance, discipline, counseling, and any ADA information that is collected and used in various areas of the College.

Approval Authority/Monitoring Authority: Piedmont Community College's Board of Trustees has approval authority for this policy. The Vice President, Administrative Services/CFO and the Vice President, Information Technology/CIO have monitoring authority for this policy.

Procedure:

Section 1: Security Protocols

1.1. PCC is often involved with activities that require compliance with the FTC (Red Flag Rules). These activities may include:

1.1.1. utilization of deferred payment plans as authorized by 1E SBCCC 200.2

1.1.2. issuance of any scholarship which requires the recipient to sign a promissory note

1.1.3. maintaining an account for student from which the student can authorize payments for goods and services such as books and food

1.1.4. using debit/credit card accounts

1.1.5. attempts to access academic or financial information

1.2. The dean or director from each high-risk area in item 1.1 is responsible for ensuring best practices are maintained when handling sensitive information and will monitor systems to identify red flags that occur.

1.2.1. Once a red flag is suspected, the dean or director should immediately contact the College's Vice President, Information Technology/CIO.

1.3. PCC's data and records management systems are protected by physical and technical safeguards which follow state and federal guidelines.

1.3.1. ITS is responsible for establishing security protocols in the retrieval of electronic information.

1.3.2. Data owners are responsible for the security and confidentiality of student information and records in each of their respective areas.

1.3.3. All PCC employees are responsible for the security of student information related to their assigned duties and for following campus-wide procedures in managing digital and hard copies of student records and information.

1.4. Each area of the campus that handles student records should establish procedures to protect the security and confidentiality of student information, including hard copy and digital formats.

1.4.1. The NC State Board of Community Colleges Code (SBCCC), General Statutes, FERPA (Family Educational Rights and Privacy Act), Federal Financial Aid Guidelines, and other state and federal guidelines must be followed in handling student information and should be addressed in the procedures for each area.

Section 2: Preventing Identity Theft

2.1. When a person does not provide any identification or provides insufficient identification, an assigned representative will follow established procedures to substantiate that person's identity.

2.2. The College will ensure employees are reminded annually about FERPA requirements to contribute to the prevention of identity theft.

2.3. Third-party agencies that handle sensitive data for the College will be evaluated to ensure they comply with best practices in information security.

2.4. All employees will adhere to FERPA laws concerning verification of proper identity and non-disclosure of data to unauthorized persons.

2.5. All banking information will be obtained and used only by appropriate personnel with PCI compliance regarding security of banking information.

2.6. Students applying for financial aid awards will be verified with more than one identification method to assure that aid is distributed to the proper person.

Legal Citation: Fair and Accurate Credit Transactions Act of 2003 (FACTA) – Public Law 108-159; N.C.G.S. 75 Article 2A; 1E SBCCC 200.2

History: Effective January 2012; revised September 2021, May 2022—updated definitions, September 2023

Cross-references PCC Policies 5.7.1 Employee Personnel File and 7.6 The Family Educational Rights and Privacy Act of 1974.