3.14 Identity Theft Prevention Program

Last Revised: January 2012

Policy: It is the policy of the Board of Trustees of Piedmont Community College to enact reasonable procedures to protect students and college employees from damages associated with the compromise of sensitive personal information.

Purpose/Definitions:

Purpose: Piedmont Community College (PCC) adopts this Identity Theft Prevention Program to enact reasonable policies and 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.

Covered account – An account with a creditor used by individuals, families, or households which involves multiple payments to that creditor. Examples include emergency loan accounts, scholarships which could involve repayment if the terms of the scholarship are not met, and deferred payment accounts approved by a college’s trustee.

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.

Identifying information – Information which alone, or in combination with other information, can be used to identify a specific individual. Identifying information includes name, social security number, date of birth, driver’s license number, identification card number, employer or taxpayer identification number, biometric data, unique electronic identification numbers, address or routing code, or certain electronic account identifiers associated with telephonic communications.

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

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 in order to thwart identity theft associated with new and existing accounts.
Sensitive information – Personal information belonging to any student, employee, or other person with whom the College is affiliated.

Service provider – Person providing a service directly to the financial institution or creditor.

Student records -- Student records are defined as 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 has monitoring authority for this policy.

Procedure: Piedmont Community College is often involved with activities that require compliance with the FTC (Red Flag Rules). These activities include:

- utilization of deferred payment plans as authorized by 23 N.C.A.C. 02D.0201(b),
- issuance of any scholarship which requires the recipient to sign a promissory note,
- maintaining an account for student from which the student can authorize payments for goods and services such as books and food,
- using debit card accounts, or
- attempts to access academic or financial information.

The Controller will assign a representative from each high-risk area to identify what red flags may exist in their department that will cause concern. Once those areas are identified, a procedure will be established to describe the College’s plan of action for investigating and resolving any breach of information. PCC will test its Identity Theft Prevention Program periodically to make sure it is working as intended. For staff training, PCC will consider the training needs for multiple campus locations, multiple records, multiple account managers, and adjunct instructors.

Piedmont Community College’s data and records management systems are provided for the purpose of conducting PCC business and instruction. The administrative, technical, and physical safeguards in accessing, collecting, distributing, processing, protecting, storing, using, transmitting, and disposing of student information and records are established by each office that uses student records. These safeguards will follow state and federal guidelines to provide security and confidentiality of all student records and information.

The Management Information Systems (MIS) Office is responsible for establishing security protocol in the retrieval of electronic information. The Vice Presidents are responsible for the security and confidentiality of student information and records in each of their respective areas. 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.

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. The NC Administrative Code and 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.

The following guidelines must be followed when accessing confidential information and student records:

**Hard Copy Data**

1. Student information with social security numbers and birth dates will not be placed on hard copy file folder labels: use the student ID number instead.
2. Student information with social security numbers and birth dates will not be left unattended on desks to which unauthorized people may have access.
3. File folders (hard copies) containing student information with social security numbers and birth dates must be kept under lock and key with access available only to authorized personnel.
4. Any documents containing confidential student information must be shredded before discarding.

**Electronic Data**

1. Electronic student data and confidential information is available only to authorized personnel in accordance with policies and procedures approved by the Management Information Systems Office.
2. Access to information systems is given to authorized personnel only with written permission by a staff member’s supervisor. Permission records will be maintained by the MIS office.
3. Personnel who have been granted authority to access student information will be issued an ID and password by the MIS office to access information systems.
4. Staff will use only their designated ID and password to access student and confidential information. Under no circumstances will an ID and password be shared or will staff members access PCC information systems using an ID and password that has not been issued to them.
5. Student information with social security numbers and birth dates will not be distributed or transmitted through e-mail or posted on networks.
6. The student ID number generated by the college operating system will be used in place of the social security number for identification purposes and in all communications.
7. Student social security numbers or birth dates may not be used for access to any student records or e-mail accounts: only the student ID number may be used.
8. MIS reserves the right to revoke all privileges to information systems if PCC Management Information Services policies and procedures are not followed.

**Student Communications**

1. Students are required to create a unique password upon setting up their accounts in PCC information systems such as Blackboard or e-mail.
2. When communicating with students regarding technical support, registration, transcripts, financial aid, and financial information, College employees will not ask students for a social security number or birth date within hearing distance of other people.
3. Two forms of authentication must be requested when verbally verifying student identification. Appropriate forms of authentication are the student Colleague ID number, the last four digits of the social security number, and the birth date. Under no circumstances should students be requested to verify their social security number through e-mail.
Identifying Potential Red Flags

1. Due to the existence of multiple locations, multiple records, multiple account managers, and multiple off-campus instructors who collect demographic information, employees should be aware that the security of sensitive data included on a variety of documents in these multiple locations could be compromised, e.g., registration forms.

2. To assist in collecting accounts, PCC contracts with many outside agencies, such as agencies that provide services for payment plans, and public or governmental collection agencies. The College provides these agencies with sensitive student data.

3. The Controller or assigned representatives will verify students during registration to assure that the correct student is being registered for courses. Issues that may arise include registering a student incorrectly when multiple students in the College database have the same name, fraudulently using an inactive account to obtain financial aid and/or student benefits, and students attempting to register after an extended absence from campus.

4. Employees sometimes save students’ or employees’ sensitive data to flash drives or laptops, a practice that may compromise the security of the data in cases of loss or theft. PCC should consider addressing the use of flash drives and laptops when developing the Identity Theft Prevention Program.

5. Phone-in payments may risk compromising bank account information.

Minimizing Red Flags

1. The Controller or assigned representatives will define the specific information to be considered “sensitive” information and will identify those areas of the campus involved in the acquisition, use, and storage of such information.

2. The Controller or assigned representatives will determine if sensitive data is being securely stored and handled, and how sensitive information is being disseminated.

3. Banking information will be handled only by authorized personnel at PCC.

4. The Controller or assigned representatives will establish proper procedures for verifying the identity of students and new employees.

5. The Controller or assigned representatives will identify third party agencies that handle student or employee accounts on behalf of the College and determine whether and how those agencies protect the sensitive data of their customers. Privacy policies from these agencies are on file in the Business Office.

6. The Controller or assigned representatives will develop a process to identify students who have registered again after a long period and who did not undergo the readmission process.

7. The Controller or assigned representatives are vigilant in dealing with security breaches in information systems such as lost or stolen portable computers, computer and network security attacks, and data files (e.g. extracts) discovered to be open to the public or to unauthorized staff.
Detecting Red Flags

1. Procedures are in place to verify a person’s identity when processing any activity to their account, including, but not limited to, registration activity, financial aid processing, bookstore transactions, and business office payments or inquiries.
2. Receipt of red flag notifications from service providers, e.g., a discrepancy between an individual’s social security number and name, or address differences, will be disseminated to appropriate College employees.
3. Notification of suspicious activity by students, law enforcement, or financial aid recipients will be disseminated to specific individuals.
4. Reports from security officers or the equipment inventory coordinator concerning the loss or theft of computers storing sensitive data will be disseminated on an as-needed basis.
5. The Controller or assigned representatives will audit changes to sensitive information, e.g., name changes or SSN changes.
6. The Controller or assigned representatives will issue a report listing students who have re-registered after an extended interruption in attendance.
7. The Controller or assigned representatives will perform routine diagnostics on firewalls and the security of electronic data portals.
8. Security scans and unscheduled scans will be run at regular intervals to detect security breaches.

Preventing Identity Theft

1. When a person does not provide any identification or provides insufficient identification, the Controller or assigned representatives will have procedures in place to substantiate that person’s identity.
2. The Controller or assigned representatives will ensure that college employees have training on FERPA to contribute to the prevention of identity theft.
3. The Controller or assigned representatives will view each off-campus registration site (including sites which are not college-owned) to determine the needs of each site regarding security of data.
4. Third-party agencies that handle sensitive data for the College will be evaluated no less than annually to ensure that they are in compliance with red flag rules.
5. All employees will adhere to FERPA laws concerning verification of proper identity and non-disclosure of data to unauthorized persons.
6. All banking information will be obtained and used only by appropriate personnel with PCI compliance regarding security of banking information.
7. A re-admission process will be in place to verify a student’s identity when an account has been inactive for a prolonged period, as determined by the applicable area.
8. Students applying for financial aid awards or loans will be verified with more than one identification method to assure that aid or loans are distributed to the proper person.
9. If the College’s bookstore buys books from students at the end of the semester, procedures will be in place to verify the identity of the student obtaining the cash. This procedure, in correlation with security reports of alleged book thefts, will be used to identify attempts to sell stolen books. If anything seems questionable about the student selling the books, bookstore personnel must verify courses taken by the student within that semester to verify that the books are valid for the student’s course enrollment.
10. Procedures will be in place on the proper handling of data, including electronically saved data on laptops or flash drives and data that are accessed remotely. This includes specifying what data
should be stored on these devices and what security measures should be taken to prevent loss or theft of such data.

11. The Controller or assigned representatives will maintain Payment Card Data Security Standard Compliance on portals where payments are received electronically in an effort for prevention and mitigation of red flags.

12. The Controller or assigned representatives will train employees, then review and test procedures for dealing with sensitive information and with access requests.

13. The Controller or assigned representatives will review internal access to paper, electronic documents, and information systems containing sensitive information.

14. The Controller or assigned representatives will have regular, mandatory staff meetings to educate employees about the risks and liabilities of data loss or theft.

Responding to Red Flags

1. The Controller or assigned representatives will ask for validation or supplemental documentation or identification when a student’s identity is in question.

2. The Controller or assigned representatives will check credit card receipts when possible fraudulent charges are reported from a customer’s bank statement.

3. The Controller or assigned representatives will verify original student documents when a discrepancy is reported regarding social security number discrepancies to name and other red flag issues regarding aged accounts.

4. The Controller or assigned representatives will deny access to information or disable an account pending further investigation and resolution of suspicious activity.

5. The Controller or assigned representatives will follow-up on reported thefts which possibly involve the compromise of sensitive data.

6. The Controller or assigned representatives will develop a plan for notifying victims of possible identity theft and proper authorities.

7. The Controller or assigned representatives will develop a plan for using all available media to disseminate information concerning an improper disclosure of sensitive information. The records of current students, former students, and employees will be considered when disseminating the information concerning a breach.

The Controller or assigned representatives will update the Identity Theft Prevention Program annually, evaluate what technologies are available to assist in combating identity theft, and consider what other policies may have changed in determining updates to the Identity Theft Prevention Program.

Legal Citation: Fair and Accurate Credit Transactions Act of 2003 (FACTA) – Public Law 108-159.

History: Effective January 2012