TOPIC: Information Technology Security - Procedures

Policy Number: F22

The goal of Cloud County Community College's Information Technology Security procedures is to define the process of compliance with the Federal Trade Commission's Safeguards Rule for the Gramm-Leach Bliley Act and the Red Flags Rule.

Gramm-Leach Bliley Act – Mandates that colleges:

- Designate an individual to oversee and enforce the information security program
- Conduct a risk assessment of likely security and privacy risks
- Institute a training program for employees who have access to covered data and information
- Evaluate and adjust the Information Technology Security program periodically.

Responsibilities

Table 1: Role Definitions and Responsibilities

Title or Role	Responsibilities
Director of Information Technology	Maintains and enforces this policy and is the point of contact for financial information
Coordinator of Institutional Research	Assists in maintenance and enforcement of this policy; provides direction for hands-on installation, maintenance, updates, and modifications of network and physical systems connected to this policy.
End User	Any employee, contractor, or trustee who accesses the college network or systems containing college data, including student employees. End users have specific responsibilities for protecting college systems and data.
IT and Data Professionals	Employees or contractors who have an elevated level of access to college network or systems. These individuals have responsibility for selecting, purchasing, deploying, maintaining, and/or disposing of college network components, systems, or digital information, and have significant security responsibilities. Examples include: Network and System Administrators, Database Administrators, and Application Administrators. These

	individuals have additional security responsibilities.
3rd Party Service Provider	Any entity that provides an information system as a service to the college that is hosted outside the college, or who hosts college data on their systems. These systems may or may not have direct integration and connectivity to the college network and systems. These 3rd party systems and organizations must minimally provide equivalent protection to that provided by the college network and systems.

Data Classification

The confidentiality and integrity categorization of each system is driven by the classification of the data maintained in each system. Table 2 defines the different classes of college data.

Table 2: Classes of College Data

Data Classification	Definition
Public	Information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all employees and all individuals or entities external to the corporation. Examples include: publicly posted press releases, publicly available marketing materials, including college website, publicly posted job announcement, and social media.
Internal	Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Data is information that is restricted to personnel who have a legitimate reason to access it. Examples include: general academic or employment data (information on employees or college organization not covered in the Confidential Classification below), business partner information where no more restrictive confidentiality agreement exists, contracts, and student data that would be categorized by FERPA as “Directory” information also falls in this category.

Confidential	Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization is required for access because of legal, contractual, privacy, or other constraints. Confidential data have a very high level of sensitivity. Examples include: Payment Card Industry (PCI) data (credit or debit card data), university business strategy, forecasts, and other sensitive financial information, personally identifiable information, medical information or social security numbers in combination with other personal data that could be used for identity theft or that are protected by regulation (such as PHI information protected by HIPAA). (This also includes other HR information.), all student data that would be categorized by FERPA as "Protected" data also falls into this category, and information related to the physical security of college employees, students, or facilities.

System Categorization

Table 3 shows how different types of college systems are categorized, and should be used as a guideline by management, IT professionals, and 3rd party service providers in defining the specific controls required for a system based upon the guidance in NIST 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. If a system does not fit neatly into one of these definitions, the definitions of system categorization and data classification should be used to determine the appropriate categorization for the system. The college will also categorize systems not controlled by the college that reside on the college network, and work with the owners of those systems to evaluate their controls and access the level of risk to compromise of the college systems and data.

Table 3: Categorization of College Systems

Type of System	**Confidentiality**	**Integrity**	**Availability**	**Reason for the Categorization**
Point of sale, student information systems, student financial aid, and other financial transaction systems	M	M	M	These systems carry confidential data (student protected information or credit card information), and must be available for college operations

HR Systems	M	M	L	These systems carry confidential data (personal information), but short outages will have minimal impact on operations
Finance Systems (general ledger, accounts receivable/payable, etc.)	L	L	L	These systems generally only carry internal data, and short outages will have minimal impact on college operations
Physical Security Systems	L	M	M	These systems may not carry confidential data, but compromise of their integrity or availability could present a significant physical risk to employees or students
Building Management Systems	L	L	M	These systems do not carry confidential data or carry internal data where this is significant integrity risk, but they have the same availability requirements as all other college operational systems
General Office Productivity, e-mail and other back office support, file storage systems	M	M	L	These systems may contain confidential data, but short outages will have minimal impact on operations
Systems or Applications Carrying ePHI	M	M	L	These systems would by definition carry confidential data, but given the college is not a health care provider, short outages would have minimal impact on operations
Network and Security Infrastructure	M	M	M	The underlying infrastructure must meet the high water mark of all systems supported by IT.

Legend

H = High
M = Medium
L = Low

Red Flags Rule:

- Requires colleges to implement a written Identity Theft Prevention Program to detect warning signs – or red flags – of identity theft in day-to-day operations.

The College's Identity Theft and Red Flag Program shall include reasonable procedures and processes designed to:

1. Identify relevant Red Flags for covered accounts and incorporate ways to handle those Red Flags into the program.
2. Detect Red Flags that have been discovered in the program.
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
4. Ensure the program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The College has identified the following types of accounts and information:

1. Student information including FERPA covered restricted information
2. Deferment of tuition payments
3. Electronic fund transfer account numbers and other bank related information
4. Credit and Debit card information
5. Short term student emergency loans
6. Financial aid refunds
7. Social security numbers
8. Personnel files

Administration of the Program

1. The Director of Information Technology shall be responsible for the development, implementation, oversight and continued administration of the Program.
2. Appropriate staff will be trained, as necessary, to effectively implement and monitor the program.
3. Appropriate and effective oversight of any external service provider shall be incorporated within the program.

Categories of Red Flags

Examples of Red Flags discovered in the program are as follows:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.
2. The presentation of suspicious documents or personal identifying information.

3. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
4. Notices of address discrepancies.
5. Recent increases in the volume of new inquiries or patterns of activity that are inconsistent with prior history.

Identification of Red Flags

The program shall address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts by:

1. Obtaining identifying information about, and verifying the identity of a person opening a covered account.
2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.
3. Limit access to information to only those legitimately need to know the information.
4. All files for employees, students and others shall be in locked filing cabinets and offices shall be locked when not occupied.
5. All documents containing protected information shall be shredded and disposed of in a secure way.

Response to Detected Red Flags

Appropriate responses to detected Red Flags to prevent and mitigate identity theft should be taken. The response shall be commensurate with the degree of risk posed.

Appropriate responses may include but are not limited to:

1. Monitor a covered account for evidence of identity theft.
2. Contact the customer.
3. Change any passwords, security codes or other security devices that permit access to a covered account.
4. Reopen a covered account with a new account number.
5. Close or place a hold on an existing covered account.
6. Notify appropriate college officials or law enforcement.
7. Determine no response is warranted under the particular circumstances.

The program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the College from identity theft.

TOPIC:	Policy Number:
Information Technology Security - Procedures	F22

Oversight of the program shall include

1. Assignment of specific responsibility for the implementation of the program.
2. Review of any reports that may be developed by staff regarding compliance.
3. Approval of material changes to the policy or procedure related to the procedures to address changing risks of identity theft.
4. Taking steps to ensure the activity of any third-party service provider engaged by the College has reasonable policies and procedures in place to detect, prevent, and mitigate the risk of identity theft in conjunction with the College's covered accounts.