# Lurleen B. Wallace Community College Information Security Program

Approved by Executive Council 1-7-2020

Updated 9-23-20

# Contents

## *1 INTRODUCTION*

Information Security is the subject of many state and federal laws. These laws and regulations create an emerging legal standard for obligations on the part of Lurleen B. Wallace Community College (LBWCC) to protect the data we collect, store, process, use, and disclose. Also, these laws affect how we handle personal information, which includes sensitive health and financial data.

Today information security is necessary to protect not only the College, but also homeland security. Institutions of higher education, like LBWCC, must also be protected from cyber-attacks. Any Information Security Program (ISP) should be designed to protect information and critical resources from a wide range of threats in order to ensure continuity, minimize risk, and ensure the availability of information.

In an effort to set safeguarding standards the Gramm-Leach-Bliley Act directs that all financial institutions implement an Information Security Program and designate a program coordinator.

The Information Security Program must include five main elements:

1. Designation of an employee or employees as coordinator of the Information Security Program.
2. Identification of internal and external risks to the security and confidentiality of customer information and evaluation of current safeguards.
3. Employee training.
4. Oversight of service providers.
5. Evaluation of the Information Security Program.

## *2 PURPOSE*

The purpose of this plan is to protect, to the extent reasonably possible, the privacy, security, and confidentiality of personally identifiable financials records and information as well as the reputation of the College.

The program applies to all personally identifiable financial records regardless of where they reside and covers employees and all other individual or entities using these records and information for any reason. The program also establishes an expectation that members of the College community act in accordance with this program, relevant laws, contractual obligations, and the highest ethical standards.

## *3 SCOPE*

This plan covers the entire LBWCC community, including students, faculty, staff, alumni, temporary employees, contractors, and volunteers and guests who have access to LBWCC information and technology resources. Examples of these resources may include data, images, text, and software, stored on hardware, paper, or other storage media.

## *4 DEFINITIONS*

*Confidentiality* - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of *confidentiality* is the unauthorized disclosure of information.

*Integrity* - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of *integrity* is the unauthorized modification or destruction of information.

*Availability* - Ensuring timely and reliable access to and use of information. A loss of *availability* is the disruption of access to or use of information or an information system.

*Risk Assessment* - A process which determines what data, information, and resources exist that require protection, and to understand and document potential risks from Information Technology security failures that may cause loss of information confidentiality, integrity, or availability.

*Control Activities* - Are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out.

*Information Assets*- Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the College.

*Network Security* - Is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.

*Computer Security*- Is concerned with the risks related to computer use, and ensures the availability, integrity and confidentiality of information managed by the computer system, permitting authorized users to carry out legitimate and useful tasks within a secure computing environment.

*Data Custodians*- Data Custodians are institutional designees who have planning and policy making responsibilities for institutional data and the institutional Data Warehouse. The Data Custodians, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability. Data Custodians are responsible for the oversight of Personally Identifiable Information (PII) in their respective areas of institutional operations.

*Personally Identifiable Information (PII)*- Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to specific individual, such as date and place of birth, mother's maiden name, etc.

*Timely Manner-* Is subjective and relative to the decisions made by the department heads based on need, time and urgency. *Timely Manner* may not be quantifiable in all instances and is up to each department head to determine the requirements needed to fulfill a timely update.

*VPN* (Virtual Private Network) - A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the College's network. VPN's use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

## *5 INFORMATION SECURITY PROGRAM*

Lurleen B. Wallace Community College is committed to meeting the Safeguards Rule of the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to develop and maintain a security plan to protect the confidentiality and integrity of personal information.

LBWCC's Information Security Program ensures that administrative, technical, and physical safeguards are implemented by the College to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered data, information, and resources in compliance with the FTC's Safeguards Rule (16 C.F.R. Part 314), promulgated under the GLBA. These safeguards are provided to:

- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

This document and all associated policies have been established to create our Information Security Program, improve the effectiveness of IT operations, satisfy any regulatory requirements, and ensure the confidentiality and integrity of our covered data, information, and resources.

### *5.1 Information Security Program Coordinator(s)*

The overall coordinator of the Information Security Program at Lurleen B. Wallace Community College is the Associate Dean of Instructional and Information Technology. The program coordinators for the Gramm-Leach-Bliley Act are the Director of Financial Aid and the Director of Admissions and Records.

The Director of Financial Aid and the Director of Admissions and Records are responsible for maintaining a program of periodic training and awareness related to the handling and protection of information covered by this Program and for overseeing service providers and contractors.

The Associate Dean of Instructional and Information Technology will assist the Director of Financial Aid and the Director of Admissions and Records with a periodic risk assessment that will identify likely security and privacy risks to the covered data, information, and resources and provide a remediation plan for the identified risks. The Director of Financial Aid and the

Director of Admissions and Records will maintain the articles related to periodic risk assessment and maintain training and awareness data provided to each relevant business unit.

The Director of Financial Aid and the Director of Admissions and Records are responsible for maintaining their respective functional unit data, and ensuring training and awareness. The Director of Student Financial Aid, the Director of Admissions and Record, and the Associate Dean of Instructional and Information Technology will evaluate this Information Security Program annually or whenever there has been as risk identified to make appropriate adjustments.

### *5.2 GLBA Committee*

The GLBA Committee exists to ensure that this Information Security Program is kept current and to evaluate potential policy or procedural changes driven by GLBA. This committee includes the following individuals: Director of Admissions and Records, Director of Financial Aid, Associate Dean of Instructional and Information Technology, Chief Financial Officer, and the Dean of Student Affairs. Other individuals may be added as needed. This committee meets annually and as needed.

Questions regarding the GLBA impacts on business processes and policies should be directed to the Coordinator of the GLB Information Security Program.

### *5.3 Risk Assessment*

Risk assessments should identify what covered data, information, and resources exist and how we plan to protect against the potential risk from Information Technology security failures and/or the loss of confidentiality, integrity, and availability. The results should help guide and determine what priorities the College will establish for managing the information security risk and how controls will be implemented to protect against the physical security, network security, and information systems.

Objectives are required and must be established before administrators can identify and take necessary steps to manage risks. Once the risks have been identified and controls are put in place, this will help to ensure that safeguards are in place to prevent most security risks. All information systems have operational and technical manuals for assisting with providing safeguards to protect the confidentiality, integrity, and availability of the covered data, information, and resources.

The Associate Dean of Instructional and Information Technology, the Director of Financial Aid and the Director of Admissions and Records shall periodically conduct and document risk analyses consisting of, but not limited to, the following:

- Asset Inventory –servers, desktops, and applications that contain covered data
- Threat assessments, including but not limited to, the following:
    - Compromised system security as a result of system access by an unauthorized person
    - Deliberate network-based attacks or malicious software upload
    - Ransomware, rendering covered data unreadable or unusable
    - Interception of covered data during transmission

    - Loss of covered data integrity
    - Inadvertent data entry
    - Physical loss of covered data in a disaster (floods, earthquakes, tornados, electrical storms, etc.)
    - Inaccessibility of covered data due to environmental factors (long-term power failure, pollution, chemicals, and liquid leakage)
    - Errors introduced into the system
    - Corruption of data or systems
    - Unauthorized access (intentional and unintentional) to electronic or hardcopy covered data, information and resources by employees or others
    - Unauthorized requests for covered data
    - Unauthorized transfer of covered data through third parties
    - Third party vendors who process covered data not appropriately safeguarding covered data
    - Unsecure storage of covered data
    - Failure to dispose of covered data in a secure manner
- Design, implementation, and development of a risk mitigation strategy
- Maintain a written record of risk assessments and remediation

The College understands this is not a complete list of the risks associated with the protection of information systems. Since technology is not static, new risks are created regularly. Therefore, the Information Technology Department will continue to monitor industry sources and advisory groups such as the Educause Security Institute, the Internet2 Security Working Group, and SANS for identification of new risks.

The College believes current safeguards are reasonable and, in light of current risk assessments, are in line with common practices to provide confidentiality, integrity, and availability for our covered data, information, and resources. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information. However, the College cannot guarantee the unequivocal security of covered data, information, and resources given the evolving and ever-changing state of Information Technology environments and threats thereto.

### *5.4 Control Activities*

Control activities are policies, procedures, techniques, and guidelines that help ensure the College's response to reducing risks that were identified during a risk assessment. The primary objective for having these control activities is to minimize the risk. If an assessment is done and the findings reveal a risk to achieve an objective, then control activities are defined and implemented.

Control activates occur throughout the College, in all departments, levels, and functions. These activities may include performance issues, approvals, authorizations, verification, and security of assets.

These activities normally involve having a policy established and then procedures to accomplish the policy. These control activities are in place to safeguard the

confidentiality, integrity, and availability of our covered data, information, and resources.

### *5.5 Information Classification*

Information Classification is required to determine the sensitivity and criticality of all data, information, and resources. All information covered by this plan is classified into one of three categories, according to the level of security required. These categories are defined as "Confidential", "Internal Use Only", or "Public".

#### *5.5.1 Tier I - Confidential*

Confidential information includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access. Unauthorized access to personal confidential information could cause an invasion of privacy as well as possible financial risks. This type of unauthorized access could also negatively impact College finances and resources. Examples of personal confidential information include social security numbers, dates of birth, medical records, credit card information, bank account information, etc. These types of personal confidential information are protected under privacy laws including the Family Educational Rights and Privacy Act and the Gramm-Leach-Bliley Act. Confidential data is intended solely for use within LBWCC and is limited to those employees that have been provided specific access based on their job responsibilities.

#### *5.5.2 Tier II - Internal Use Only*

Internal Use Only information includes information that is less sensitive than confidential information, but that if exposed could cause financial loss or damage to LBWCC's reputation, or violate an individual's privacy right. Examples of this type of data for the institution perspective could be internal memorandums meant for limited exposure or draft documents subject to internal comments before public release.

#### *5.5.3 Tier III - Public*

Public information is information that is not publicly disseminated, but accessible to the general public. This type information should not have any adverse effects on the individual members of the College or the operations, finances, or reputation of the College.

### *5.6 Documented Safeguards Program:*

#### *5.6.1 Employee Management and Training*

Reference checks are conducted for all new full-time employees at LBWCC that are working in areas that regularly work with covered data, information, and resources (e.g.,

Information Technology Department, Business Office, Admissions and Records, Financial Aid, Human Resources).

LBWCC also has a new employee orientation that is provided by the Human Resources department to the appropriate supervisor of the new employee. During employee orientation, new employees have a checklist that must be completed. The checklist has steps that require their supervisor and the employee to ensure that they have completed all the necessary forms in HR; met with the Business Office to have keys assigned based on their access to their office or specific locations; and meet with the Payroll office to sign all forms, discuss sick leave bank procedures, and access payroll and leave information on the web portal. The supervisor also works with the employee and IT to set up a domain account; create an email account; and create credentials giving access to information systems based on their job responsibilities. The new employee must sign and date the checklist form and return it to human resources.

This process ensures that the new employee has the necessary documents, access and resources needed for them to be successful in their new role at the College.

Employees in relevant functional units receive additional training regarding the importance of safeguarding the confidentiality, security, and integrity of covered data (e.g. student records, student financial information), including the College's Policy on Confidentiality of Student Records (FERPA) and regulations from the Department of Education.

These employees are also trained on security measures, including the proper use of computer information and passwords and incident response and breach notification procedures. Reports of these training efforts, which help minimize risk and safeguard covered data, information, and resources, are provided to the Director of Student Financial Aid and the Director of Admissions and Records.

### *5.6.2 Physical Security*

The College has addressed physical security by placing access restrictions at buildings and computer facilities containing information resources to permit access only to authorized individuals. These locations are to be locked at all times, and only authorized employees are permitted to possess keys. These measures are used to safeguard the covered data, information, and resources.

In facilities containing covered data, information, and resources, there are cameras, alarms, redundant power systems, fire detection and suppression systems, and other safeguards, as appropriate, to discourage and respond to unauthorized access.

### *5.6.3 Information Systems*

Access to covered data, information, and resources via the College's IT Infrastructure is limited to those employees who have job responsibilities that require access to that information. The information system is updated when updates are released to the College by Alliant. These updates are reviewed by a committee and then a request is made to Alliant

to install the update. The covered data, information, and resources are securely stored in a central location that requires a key to access the physical location.

The Information Technology Department uses all technological products available to ensure that all covered data, information, and resources are securely stored. Authentication is also required of users before they can access College protected data. In addition, security systems have been implemented to assist with detection and mitigation of threats, along with procedures to handle security incidents when they do occur. When reasonable, encryption technology will be utilized for both storage and transmission. All covered data, information, and resources will be maintained on servers that are behind a firewall.

Network security is defined under operations management in section 5.9.

### *5.7 Information Handling*

College employees create many records daily as part of normal business. These types of records contain highly sensitive information and should be maintained under strict controls as outlined in this document. Mishandling of records could case great risk to the College and financial and reputational harm to an individual. It is the process of LBWCC that we protect sensitive information and those that access this data. Specific controls are in place to ensure the protection of highly sensitive data information.

### *5.8 Identity and Access Management*

Identity and access management ensures that LBWCC has accurate identification for all student, faculty, staff, guest, and community members when accessing network-based services. Identity and access management is based on principles and control objectives.

- Ensure all student, faculty, staff, guest, and community members have unique identification when assigning access.
- Only authorized personnel will have access to covered data, information, and resources.
- Provide periodic review of accounts and access.
- Use ever-changing technologies to provide effective access.

Access control is a process that controls access to all networks, information systems, servers, computers and information based on security requirements. The goal of this plan is to ensure there is no unauthorized access to sensitive information.

#### *5.8.1 Identification*

Identification is a process the College uses to ensure all individuals and systems have a unique identifier. The key feature for this is to ensure that all students, faculty, staff, guest, and community members have a way to be uniquely identifiable.

### *5.8.2 Authentication*

Authentication is a process that determines a person is who they say they are. Authentication verifies the identity of the person against a password, token, or biometric marker. Another option for authentication is two-factor authentication. LBWCC maintains credentials for accessing networks, servers, computers, information systems and remote access as well.

### *5.8.3 Authorization*

Authorization is a process that grants permission to users that have passed the authentication process. This type of process gives a user rights to specific information. The basic types of access are read-only, create, delete, and/or modify. For LBWCC, most of these rights are granted from either credentials used to gain network access or program access in the information system.

### *5.8.4 Remote Access*

Remote access to covered data, information, and resources is only granted through secure, authenticated methods. LBWCC uses a secure VPN connection for employees to access resources or confidential information remotely. The access credentials for remote access require a unique username and password.

## *5.9 Operations Management*

System communication protection ensures that covered data, information, and resources are available and secure when users are trying to do their jobs. The appropriate level of security applied to these types of resources are based on the level of sensitivity. The key elements of operations management are network security, security monitoring, virus protection, and backup and recovery.

### *5.9.1 Network Security*

Most network attacks launched from the Internet on College networks can cause major damage to network devices, computers, and covered data and information. In order to provide counter measures against these type of attacks, firewall and network filtering technology must be used in an organized and consistent matter.

LBWCC uses appropriate network security protocols and network security controls to try and safeguard against this type of attacks on our covered data, information, and resources. The following are some of the controls used:

- Firewall and Intrusion Detection Systems
- Firepower Server – URL Filtering for blocking malicious sites
- Anti-virus and malware software

These devices are deployed on the campus border and servers and computers to help block attacks.

### *5.9.2 Security Monitoring*

Security monitoring provides a means by which to confirm that information resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is early detection of issues and new security vulnerabilities. Early detection can prevent possible attacks and minimize impact on computer systems.

Any equipment attached to the College's network is subject to security vulnerability scans. The goal of the scans is to reduce the vulnerability of computers and the network to hacking, infection, and other security risks from both inside and outside the College. Network Administrators scan servers and network hardware to ensure these devices are safe from vulnerability.

LBWCC also does scans that are required by the Payment Card Industry Data Security Standards (PCI DSS) for credit card processing. These external scans are required every 90 days and you must successfully pass each scan. The College is also required to complete the SAQ D yearly.

The College also has security monitoring via video surveillance at each location.

### *5.9.3 Virus Protection*

Viruses are a major threat to any business or College. Antivirus software is installed on all servers and computers at LBWCC. The College uses Symantec's Endpoint Protection Manager to provide the latest updates on all connected devices to ensure the device is virus-free. The College reserves the right to review any device connected to our network for adequate virus protection.

### *5.9.4 Backup and Recovery*

All covered data and information is copied onto secure storage media on a regular basis for the purpose of recovery. The Backup Policies and Procedures state the requirements for backup and recovery. The College also has an off-site backup that backs up all covered data and information and most of the high volume file shares nightly.

### *5.9.5 LBWCC's Information Technology Acceptable Use Policy*

The College expects all students and employees to use covered data, information, and resources in a responsible manner, respecting the public trust through which they've been provided, the rights and privacy of others, the integrity of the facilities, and pertinent laws, College policies and standards, and to limit their use of data, information and resources to the educational purposes and legitimate business of the College. This policy applies to all users of the College's data, information, and resources including faculty, staff, students, guests, organizations, and individuals accessing external network services, such as the Internet via

College facilities. By using the College's data, information and resources, users agree to abide by these policies and procedures and to safeguard these assets.

All individuals are expected to make information decisions and be responsible for protecting these resources no matter the environment, shared or stand alone.

LBWCC's Information Technology Acceptable Use Policy is the governing philosophy by which individuals are expected to use our covered data, information, and resources.

### *5.10 System Failures and Compromises*

The College has documented plans and procedures to detect actual or attempted attacks on College systems and has Incidence Response plans in place which outline procedures for responding to an actual or attempted unauthorized access to covered data, information, and resources. Incidence Response and Reporting procedures are below.

### *5.11 Best Security Practices*

Following security best practices helps to decrease the risk of information security breaches**.** It is the responsibility of each member of the College community to follow the basic computer safety guidelines listed in this document. The goal of the College is to help maintain a secure computing and network environment. These best practices are a general guideline based on industry standards for information security. All employees should familiarize themselves with the following guidelines:

- Use complex passwords that can't be easily guessed, and protect the passwords.
- Beware of scams.
- Secure your area before leaving it unattended.
- Secure laptops and mobile devices at all times.
- Secure memory sticks
- Lock or log off computers or other devices before leaving them unattended, and make sure they require a password to start up or wake-up.
- Make sure your computer has adequate anti-virus software and that patches and updates are current.
- Protect portable and mobile devices.
- Don't install or download unknown or unsolicited programs to LBWCC computers.
- File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing private or confidential information should be immediately removed from the printer.
- Upon disposal, restricted and/or sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Only install apps from trusted sources.
- Keep your device's operating system updated.

- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on any device.
- Keep sensitive data (e.g., SSN's, credit card information, student records, health information, etc.) off of your workstation, laptop, or mobile devices.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.
- Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer.
- If attachments or links in an email are unexpected or suspicious for any reason, don't click on them.
- Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

### *5.12 Information Security Incident Response*

An Information Technology security incident is defined as any event that has the ability to impact the confidentiality, availability, or integrity, of the College's covered data, information, and resources. Responding to an incident effectively to alleviate any damage will determine the success of our plan. Proper handling of security incidents will provide valuable insight for the future. This type of incident could result in any of the following:

- Misuse of confidential information (SSN, grades, health records, financial transactions, etc.)
- Misuse of the College's IT infrastructure.
- Unauthorized access to College resources or information.

If an incident occurs, LBWCC has a plan in place for reporting, investigating, and resolving the incident. If employees suspect an IT security incident, they should contact the Associate Dean of Instructional and Information Technology, who will work to resolve the incident as soon as possible.

### *5.13 Oversight of Service Providers*

GLBA requires the College take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program ensures that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Director of Financial Aid and the Director of Admissions and Records will identify service providers who have or will have access to covered data, and work with Procurement and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data. The section of the College's General Terms and Conditions, entitled "Safeguarding Rules of the Gramm-Leach-Bliley Act," is accessible on the website and sets forth the specific terms contractors

of the College must comply with to maintain appropriate safeguards for covered data and information.

## *6 Regulations*

The College is proactive in being prepared to comply with a wide variety of federal and state laws, regulations, and policies with respect to information protection and privacy.

### *6.1 Family Education Rights and Privacy Act (FERPA)*

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

### *6.2 Health Insurance Portability and Accountability Act (HIPAA)*

HIPAA and its regulations (the "Privacy Rule" and the "Security Rule") protect the privacy of an individual's health information as well as govern the way LBWCC collects, maintains, uses, and discloses protected health information ("PHI").

### *6.3 Gramm-Leach-Bliley ACT*

The Gramm-Leach-Bliley Act (GLB Act or GLBA) is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written Information Security Program created by the institution.

The primary data protection implications of the GLBA are outlined in its Safeguards Rule, with additional privacy and security requirements issued by the FTC's Privacy of Consumer Financial Information Rule (Privacy Rule), created under the GLBA to drive implementation of GLBA requirements. The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

### *6.4 Payment Card Industry Data Security Standards*

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. PCI DSS provides a single approach to safeguard confidential credit card account data that the College must follow when storing, processing or transmitting credit card data.

### *6.5 Red Flag Rules – "Identity Theft"*

The Red Flags Rule defines the terms "creditor" and "covered accounts" broadly. A "creditor" under the Red Flags Rule includes any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. Although the FTC, in many contexts, does not have jurisdiction over not-for-profit entities, it has taken the position that not-for-profits are subject to FTC jurisdiction when they engage in activities in which a for-profit entity would also engage. In its July 2008 guidance, the FTC stated "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

Activities that could cause colleges and universities to be considered "creditors" under the Red Flags Rule may include, for instance:

- participating in the Federal Perkins Loan program,
- participating as a school lender in the Federal Family Education Loan Program,
- offering institutional loans to students, faculty, or staff, or
- offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.