CP 1.26.1
Gramm-Leach-Bliley Act
Required Information Security Program

Related Board of Trustee Policy: BP 1.26

Responsible Official	*Vice-President for Finance and Administration* *Director of Technology*
Approvals	*09/10/2020*
Revision	

Procedure

I. Purpose

The Gramm-Leach-Bliley Act ("GLB"), together with an implementing Federal Trade Commission ("FTC") "Safeguards Rule," regulates the security and confidentiality of customer information collected or maintained by or on behalf of financial institutions or their affiliates. Because McDowell Technical Community College is classified as a financial institution under GLB, by virtue of processing or servicing student accounts, the College has established this Information Security Plan (the "Plan") to assure compliance with GLB and the Safeguards Rule. As required by the Safeguards Rule, the Plan is designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

II. Policy Statement

McDowell Technical Community College complies with, and requires its employees and other agents to comply with, all applicable federal, state, and local laws and regulations, as well as College policies and procedures, that govern information security, confidentiality, and privacy. This Information Security Plan incorporates, by reference, future and existing College-wide or departmental policies and procedures that address the security and confidentiality of data encompassed by the definition of "covered data," below.

III. Definitions

Customer information is defined as any record containing nonpublic, personally identifiable financial information, whether in paper, electronic, or other form, that the College obtains from a student, a student's parent(s) or spouse, employee, alumnus, or other third party, in the process of offering a financial product or service; or such information provided to the College by another financial institution; or such information otherwise obtained by the College in connection with providing a financial product or service. Examples of customer information include names, addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers. In general, the financial products or services offered by a college or university include making student loans and other miscellaneous financial services as defined in 12 CFR § 225.28.

Covered data is defined as all information required to be protected under GLB. This

includes customer information, as well as financial information that the College, as a matter of policy, has included within the scope of this Plan, whether or not such information is covered by GLB. This may include financial and personal identifying information obtained by the College outside of a financial service transaction covered by GLB. Service providers are defined as all third parties who are provided access to covered data. Examples of service providers include businesses retained to transport and dispose of covered data, collection agencies, and systems support providers.

IV. Information Security Plan Components

GLB requires financial institutions to develop, implement, and maintain a comprehensive information security plan that contains administrative, technical and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information it handles. The five components of the plan require each institution to:

1. designate one or more employees to coordinate the safeguards;
2. identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of the current safeguards for controlling these risks;
3. design and implement information safeguards to control the identified risks, and ensure that the effectiveness of these safeguards is regularly tested and monitored;
4. select service providers that are capable of maintaining appropriate safeguards and require them, by contract, to implement and maintain such safeguards; and
5. evaluate and adjust the information security plan based on the results of the testing and monitoring, any material changes to operations, or any other circumstances that have or may have a material impact on the information security plan.

V. Information Security Plan Program Officer The GLB Information Security Plan Program Officer (the “Program Officer”) is responsible for implementing and maintaining this Plan. The Program Officer is the College’s Director of Technology. In implementing this Plan, the Program Officer is to work closely with the Technology Department, Student Services, Business Office, Human Resources, and all other relevant academic and administrative organizational units. The responsibilities of the Program Officer include, but are not limited to, the following:

- The Program Officer is to consult with responsible offices to identify organizational units with access to covered data, ensure that all such units are included within the scope of this Plan, and maintain a current listing of these units.

- The Program Officer is to work with all relevant organizational units to:

  - identify potential and actual risks to the security and privacy of covered data;
  - evaluate the effectiveness of current safeguards for controlling these risks;
  - design and implement additional required safeguards; and
  - regularly monitor and test the Plan.

- The Program Officer is to work with appropriate organizational units to ensure that adequate training and education programs are developed and provided to all employees with access to covered data, and that existing policies and procedures that provide for the security of covered data are reviewed and

adequate. The Program Officer is to make recommendations for revisions to policy, or the development of new policy, as appropriate.

- The Program Officer is to consult with responsible organizational units to identify service providers with access to covered data, ensure that all such service providers are included within the scope of this Plan, and maintain a current listing of these service providers.
- The Program Officer is to review the Plan, including this and related documents, annually, and make adjustments as needed. The Program Officer is to maintain a current, written Plan and make it available to the College community.

In carrying out these responsibilities, the Program Officer may require organizational units with substantial access to covered data to develop and implement supplemental information security programs specific to those units, to provide the Program Officer with copies of the program documents, and to designate responsible individuals to carry out activities necessary to implement this Plan.

VI. Risk Identification and Assessment Under the guidance of the Program Officer, organizational units with access to covered data are to take steps to identify and assess internal and external risks to the security, confidentiality, and integrity of that data. At a minimum, this process is to consider the risks to covered data, and the safeguards currently in place to manage those risks, in each relevant area of College operations including: employee management and training; information systems, including network and software design; as well as information processing, storage, transmission, and disposal for both paper and electronic records; and security management, including the prevention, detection, and response to attacks, intrusions, or other systems failures. The Program Officer is to establish procedures for identifying and assessing risks in each relevant area of the College's operations outlined above. Each affected organizational unit, in consultation with the Program Officer, is to perform the risk identification and assessment, and is to identify a responsible individual to serve as that unit's contact person with the Program Officer. Risk assessments are to include system-wide risks, as well as risks unique to each area with covered data. The Program Officer is to ensure that risk assessments are conducted at least annually, and more frequently where required.

VII. Information Safeguards and Monitoring The Program Officer is to verify that organizational units with access to covered data design and implement reasonable safeguards to control identified risks to the security, confidentiality, and integrity of that data, and that the effectiveness of these safeguards is monitored regularly. Such safeguards and monitoring are to include the following:

a. **Employee Management and Training** Safeguards for information security are to include the management and training of those individuals with authorized access to covered data. In consultation with the Technology Department and other responsible organizational units, the Program Officer is to identify categories of employees and others with access to covered data. The Program Officer is to work with Human Resources and other responsible organizational units to develop appropriate training and education programs for all affected current and new employees. These programs will be a component of the New Employee Orientation Program conducted by Human Resources. Training and education may also include brochures, web sites, and other means of increasing awareness of the importance of preserving the confidentiality and security of covered data.

b. **Information Systems** Information systems include network and software design, as well as information processing, storage, transmission, and disposal. Each affected organizational unit is to implement and maintain in writing administrative, technical, and physical safeguards to control the risks to information systems, as identified

through the unit's risk assessment process. Safeguards are to be designed and implemented in accordance with the nature and scope of a unit's activities and the sensitivity of the covered data to which it has access. The Program Officer, the Technology Department, and other responsible organizational units are to work with individual units as requested or appropriate in the design and implementation of safeguards. Safeguards may include: creating and implementing access limitations; using secure, password-protected systems, and encrypted transmissions within and outside the College for covered data; regularly obtaining and installing patches to correct software vulnerabilities; prohibiting the storage of covered data on transportable media (floppy drives, zip drives, etc); permanently removing covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media prior to disposal; storing physical records in a secure area with limited access; protecting covered data and systems from physical hazards such as fire or water damage; disposing of outdated records under a document disposal policy; and other reasonable measures to secure covered data during the course of its life cycle while in the College's possession or control.

c. **Security Management and Managing System Failures** In consultation with the Technology Department and other responsible organizational units, the Program Officer is to develop and implement effective procedures for preventing, detecting, and responding to actual and attempted attacks, intrusions, and other systems failures. Such procedures may include implementing and maintaining current anti-virus software; maintaining appropriate filtering or firewall technologies; regularly obtaining and installing patches to correct software vulnerabilities; imaging documents and shredding paper records; regular data back up and off site storage; implementing incident response plans; and other reasonable measures. The Program Officer, working with the Technology Department, is to assist affected organizational units in implementing the appropriate security management procedures. The Program Officer may elect to delegate to an appropriate individual in the Technology Department responsibility for monitoring and disseminating information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the College.

d. **Monitoring and Testing** In consultation with the Technology Department and other responsible organizational units, the Program Officer is to develop and implement procedures to test and monitor the effectiveness of information security safeguards. Monitoring levels are to be appropriate to the probability and potential impact of the risks identified, as well as the sensitivity of the information involved. Monitoring may include sampling, systems checks, systems access reports, and any other reasonable measures adequate to verify that Plan safeguards, controls, and procedures are effective.

VIII. Service Providers and Contract Assurances

The Program Officer, by survey or other reasonable means, is to identify service providers with access to covered data and the organizational units that provide this access. Working with these units, the Program Officer is to ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for covered data, and are to require service providers, by contract, to implement and maintain such safeguards. Working with the Business Office, the Program Officer is to develop and send to each covered service provider a form letter that requests assurances of GLB compliance. The Business Office is to take steps to ensure that all relevant future contracts incorporate a "GLB compliance clause" that requires service providers to implement and maintain safeguards for covered data.

IX. Periodic Review and Adjustment of Plan

The Program Officer, working with the Technology Department and other responsible organizational units, is to evaluate and adjust annually the Plan in light of the results of

the testing and monitoring described in paragraph (3)(d), above, as well as any material changes to operations or business arrangements, including changes in technology, the sensitivity of covered data, and the nature of internal and external threats to information security, and any other circumstances that may reasonably impact the Plan.

The Program Officer, in consultation with the VP of Finance and Administration, is to review the Plan annually to assure ongoing compliance with GLB and the FTC Safeguards Rule, as well as consistency with other existing and future laws and regulations.

Note: Label all your controls with a control reference number in the above narrative. This control reference number will be cross-referenced throughout the remainder of the templates.

A critical control is a control that will prevent or detect an error in the event that all other controls fail. If there isn't a critical control in the process you may need to test all the controls in your narrative. If the critical control encompasses the prior controls you will only need to test the critical control and not the individual control.

Refer to the Guidance Manual and/or Case Studies for an example of how to complete the narrative template. The narrative should be for the process in place at the end of the current fiscal year. If your College's processes are changing during the fiscal year, document the new process that will be in effect at the end of the current fiscal year, rather than the old process.