MOTLOW STATE COMMUNITY COLLEGE

POLICY

Category
INFORMATION SECURITY PROGRAM (GRAMM, LEACH, BLILEY) – 1:08:00:02
Approval
Leadership Council Approved: January 30, 2015
Effective Date/Approved: January 30, 2015
Revised: January 13, 2015; editorial changes made September 2, 2016
Responsible Party: Chief Information Officer

Table of Contents

A. INTRODUCTION

On May 23, 2003, the Federal Trade Commission adopted the "Standards for Safeguarding Customer Information" Rule promulgated under the authority of the Gramm-Leach-Bliley Act (GLBA). The GLBA safeguarding rule requires all financial institutions, including institutions of higher education, to develop and draft a comprehensive, written Information Security Program that includes administrative, technical and physical safeguards to protect the confidentiality of customers' nonpublic financial information that is held in the institution's possession.

According to Tennessee Board of Regents guidelines, nonpublic financial information means any information regarding a student or third party obtained in connection with providing a financial service to that person. Examples of nonpublic information include, but are not limited to, mailing addresses, phone numbers, bank and credit card account numbers, income tax records, credit histories, and Social Security numbers.
In order to comply with the Federal Trade Commission's safeguarding rule and the GLBA, Motlow State Community College has prepared this Information Security Program.

B. SECURITY RISK ASSESSMENT

Motlow State Community College's Information Security Program will "identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise of such information, and assess the sufficiency of any safeguards in place to control these risks." To this end, Motlow State Community College's will assess:

- what employees have access to nonpublic financial information
- what access they have
- what type of training is required for each employee
- what type of safeguards are needed for hard copy records and for electronic records/systems
- what type of controls are needed to detect, prevent, and respond to threats or failures of these systems

1. Employee Training and Management
   Motlow State recognizes that one of the most serious threats to the security, confidentiality, and integrity of nonpublic financial information is through errors made on the part of employees not familiar with proper procedures for handling such information. Training such employees to protect nonpublic financial information is essential to the success of the program. Consequently, annual training will be offered in an online format with content designed to satisfy GLBA re-training requirements. Once online training has been completed, the employee will certify that he or she has participated in this training. The Human Resources department will receive an email that the training has been completed. Motlow State will continue with yearly re-training requirements as required by TBR policy for all GLBA affected employees. All new employees that are deemed to need GLBA training will be informed of the GLBA online training as part of the orientation process.

2. Safeguards of Information Systems/Technology
   a. Hard Copy Records
      Motlow State recognizes that it has both internal and external risks involving hard copy records. These risks may include, but are not limited to:
      - Unauthorized access to covered data and information (i.e., mailing addresses, phone numbers, bank and credit card account numbers, income tax records, credit histories, and Social Security numbers) by someone other than the owner of the covered data and information
      - Unauthorized access of covered data and information by employees
      - Unauthorized requests for covered data and information by someone other than the owner of the covered data and information Unauthorized access to hard copy files or records
      - Unauthorized transfer/delivery of covered data and information through third parties

      Motlow State realizes that this list may not be complete. Risks associated with the protection of hard copy and covered data and information change as procedures within the college change. To this end, the college will actively monitor and/or participate in advisory groups associated with the security risks involving hard copy records.

      Presently, Motlow State assesses a need for reasonable and appropriate steps to be taken to specifically train employees who are in contact with hard copy records of covered data and information to ensure that hard copy records of covered data and information may be protected from internal and external risks.

b. Electronic Records

Motlow State's computer network consists of thousands of staff and customers, most of whom are students, stretched across the Middle Tennessee region. These users are capable of reaching all college computer resources from any of the college's campuses via data lines connected to the main campus in Lynchburg. A network the size of Motlow State's is vulnerable to many types of security breaches, virus attacks, and malicious use by unauthorized as well as authorized users. Internal network resources, servers, and computers are vulnerable to staff or student misuse by releasing a known or unknown computer virus that could infect the entire network, possibly allowing data to be easily accessed. Computer systems that lack password authentication could open confidential information to countless numbers of unauthorized users. Having networks that are commingled with many types of users can also allow unscrupulous users the ability to intercept traffic as it flows across the network as well as launch denial of service attacks at multiple systems. Other ways data integrity can be violated is simply by users sharing passwords or allowing others to access their computer session. Loss of data is always a possibility due to power failure, system failure, or user error.

3. Methods to Detect, Prevent, and Respond to Attacks, Intrusions, or other System Failures
Motlow State offers high speed Internet access to all network users at all campuses. All Internet bound network traffic must flow through the Lynchburg campus as it serves as the college's only egress to the Internet. By allowing access to the Internet, MSCC is also allowing Internet users to access its internal network. This can often lead to many of the same risks that are associated with the internal network as stated above, but those risks are multiplied due to the vastness of the Internet. Malicious users on the Internet often take advantage of vendor security flaws to attack systems and access restricted data. MSCC has identified that users from the Internet could attack college computers and servers using known and unknown software and hardware vulnerabilities or deliver virus payloads directly to a computer or indirectly via electronic mail. Having open systems available to the Internet can often lead to direct system attacks by using specialized software written specifically to locate user accounts, user passwords, system security vulnerabilities, or vendor specific system flaws.

C. IMPLEMENTATION OF SAFEGUARDS

1. Employee Training and Management
During employee orientation, each new employee from areas that work with covered data and information will be informed of the online training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee will also be trained in the proper use of computer information and passwords. Training will also include controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling," and how to properly dispose of documents that contain covered data and information. Each employee responsible for maintaining covered data and information will be instructed how the college takes steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

   Annual training will be offered in an online format with content designed to satisfy GLBA re-training requirements. Once the training has been completed the employee will certify that he or she has participated in this training. The Human Resources department will then receive an email that the training has been completed. Motlow State will continue with annual training requirements as required by TBR policy for all GLBA affected employees. All new employees will be informed of the GLBA online training as part of the orientation process.

   An overview of the employee training process is shown in Attachment A.

2. Safeguards of Information Systems/Technology
   a. Hard Copy Records
      To ensure that all Motlow State employees are in compliance with the GLBA, the following guide outlines basic measures for ensuring student hard copy records.

Information that must be protected under GLBA

- Information including, but not limited to, names, addresses, phone numbers, bank and credit card account numbers, financial information, income credit histories, and Social Security numbers.
- Directory information not associated with GLBA may be released in accordance with the Motlow State student record policy, which mirrors SACS COC guidelines in following FERPA.

Request for covered data and **information**

Covered data and information may be requested by phone or e-mail from a third party other than the owner of the data or information. It is important that any employee receiving such a request report the request for personal information to a Motlow State employee who has undergone appropriate GLBA information security training.

At times an employee may suspect that the third party requesting information is involved in "pretext calling"-which occurs when an individual improperly obtains personal information of a student with intent to commit identity theft. "Pretext callers" may pose as the student or someone authorized to have student covered data and information. The "pretext caller", in an effort to gain employee trust, may offer a piece of personal information about the student already in their possession. If it is suspected that the request for covered student data and information is fraudulent, the request should immediately be reported to the Vice President for Student Affairs, who is considered the keeper of all hard copy student data and information. An employee should never give out a student's social security number over the phone or email and never confirm covered data and information a third party caller provides.

A student's personal information may be released only if the student has specifically authorized you (the employee) to do so in a written waiver, and only if the release meets one of the stipulations covered by our internal policies that follow SACS COC and FERPA guidelines.

Daily use and storage of covered data and information

Hard copy records, printouts, forms, phone messages, etc. that contain covered data and information must also be secured. Employees should not leave any of the above materials containing covered data or information where an unauthorized person from inside or outside the institution could obtain this data. Hard copy materials containing student covered data and information should be secured in locked filing cabinets or other secured storage areas.

b. Electronic Records
   MSCC has taken proactive steps to protect the network and secure confidential information. Routine system upgrades are performed to ensure all network, server, and computer systems have the latest vendor releases. Network and server personnel routinely apply appropriate security system patches as released by the vendors. The college has implemented a domain structure where all computers are controlled centrally and require user authentication in order to logon. All shared server resources are secured by requiring user authentication. Data is further protected by allowing users the ability to view and edit data through restricted user rights. Only approved users will have read/write permissions to certain MSCC data. In order to access a system, a user must have a unique username and password and is required to change the password every 120 days in accordance to TBR Guideline G-051 and adhere to system password policies and/or guidelines. Each user must agree to follow the college's computer use policies and/or guidelines, which include not sharing usernames, passwords, or confidential information. Users are not allowed access to restricted information until properly authorized according to current policies. The college has protected against network traffic interception by implementing multiple networks on switched networking equipment. Wireless network traffic is protected by using authentication to access the wireless network, and encrypting the data to secure it from being intercepted.

   All computers and server systems are protected by anti-virus software that is automatically updated to the latest vendor releases. All electronic mail is scanned for viruses before the user has access to the message or as the message is being sent by the user. Loss of information either by system failure,

power failure, or user error is protected by having redundant server systems with multiple hard drives that are archived to tape and/or disk on a daily basis. These archived tapes and/or disks are then stored at an offsite location for a period of time as directed by current policies. All phone systems and POE switches are protected from power outages or spikes by universal power supplies and will allow the system to operate for short periods during emergencies. Motlow College's server rooms have UPS backups that will take over in case of a power outage. The college also has disaster recover policies to ensure quick recovery after a disaster.

3. Methods to Detect, Prevent, and Respond to Attacks, Intrusions, or Other System Failures
   All Internet traffic must pass through a firewall that protects all internal campus computers from direct Internet attacks. Suspect network traffic is isolated and removed from the network. To further strengthen the network from intrusion from the Internet, internal non-routable private IP addressing has been implemented. This ensures that all traffic coming from the Internet pass through the firewall and be inspected before being forwarded to any college computer system. All servers that are accessible from the Internet are isolated on a separate network to further protect confidential information. No internal network system allows direct contact from the Internet.

   The communications staff constantly monitors all systems for any indication of attacks, intrusion, or system failures. Network monitoring systems are in place that will alert staff when systems have failed and are unreachable by users. Other systems alert staff that attacks are taking place against network systems, and some systems have automatic safeguards to isolate themselves to protect the network as a whole. Other methods of detection include, but are not limited to, monitoring system logs, paging systems, and e-mail systems. Staff constantly research current trends in network and system security and attempt to implement safeguards before an attack takes place. Other safeguards include constant review of current policies and procedures and modifying those as necessary to keep current as technology changes. User accounts are periodically evaluated to make sure users are currently employed and that a user does not have access to unauthorized systems.

D. OVERSIGHT OF SERVICE PROVIDERS & CONTRACTS

The College may share customers' non-public financial information with third parties as appropriate during the normal course of business. Such business activities may include, but not be limited to, collection of accounts, transmission of documents, destruction of paper and electronic records, destruction of equipment, and other similar services. Within the framework of this Information Security Program, the College will ensure that reasonable steps are taken to secure third party contractors that are willing and capable of appropriately securing customers' non-public financial information. College contracts with third party service providers will include standard contract provisions promulgated by the Tennessee Board of Regents that require the service provider to comply with GLBA safeguarding rules in its handling of such records. Existing contracts will be reviewed; if GLBA applies, the contracts will be amended by incorporating the standard TBR amendment.

The Contracts Officer will work with the office of Business Affairs and other units as appropriate to identify third party service providers that are provided access to customers' non-public financial information. The Contracts Officer will work with appropriate campus and TBR personnel to ensure that third party service provider contracts contain language to protect customers' non-public financial information.

E. EVALUATION & REVISION OF PROGRAM

The Information Security Program will be subject to periodic review and adjustment. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the executive staff who will assign specific responsibility for implementation and administration as appropriate. The executive staff will no less than annually review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the program to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

ATTACHMENT A

Employee Training Process Overview

Motlow State will provide training on an annual basis for the employees who require training based on GLBA guidelines. The training provided by Motlow State will utilize an online self-paced presentation which will provide a certification opportunity at the end. This online training can also utilize different multimedia presentation methods that include, but are not restricted to videos, audio clips, and presentation graphics.

This training is located online via MSCC's web servers and can be accessed as directed by the Office Human Resources.