Information Security Program
(and the Gramm Leach Bliley Act (GLBA)
General Policy

INTRODUCTION

The County College of Morris recognizes and respects the importance of personal privacy for our customers. We are aware of the sensitive nature of the personal information we use in providing educational services and take reasonable precautions to protect our customer's privacy. Employees, vendors and agents of the County College of Morris (the college) have a responsibility to protect the confidentiality of all customer information.

The College is bound by state and federal laws to protect the information the customer entrusts to us. The Gramm-Leach-Bliley Act (GLBA), Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Fair and Accurate Credit Transaction Act (FACTA), and various other laws, regulations and industry standards provide the basis for the framework upon which we build our policies and procedures pertaining to safeguarding the privacy of customer information.

PURPOSE AND SCOPE

This information security program policy implements sections 501 and 505 (b)(2) of the Gramm-Leach-Bliley Act (GLBA), as promulgated under 16 CFR Part 314, to establish standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
In addition to the information required to be protected under GLBA, the College shall protect all other sensitive personal identifiable information. Collectively this information will be referred to as "Customer Information".

DEFINITIONS

Customer Information: Any record containing nonpublic personally identifiable information (PII) that is not publicly available whether in paper, electronic, or other form, that is handled or maintained by or on the behalf of the College.

Information Security Program: The administrative, technical, and physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Service Provider: Any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services with the College.

Relevant Area: Any office or department that has access to customer information.

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

The safeguards included in the College's information security program policy are reasonably designed to:
    (a) Ensure the security and confidentiality of customer information;
    (b) Protect against anticipated threats to the security or integrity of such information; and
    (c) Protect against unauthorized access to or use of such information that could result in harm or inconvenience to any customer.

POLICY ELEMENTS

(a) Designated Customer Information Security Program Coordinator

County College of Morris has designated the Director of Network and User Services as the Information Security Program Coordinator. The Coordinator is responsible for implementing and maintaining the College's Information Security Program.

The Coordinator will identify and maintain a listing of relevant areas of the College with access to customer information.

The Coordinator will ensure that risk assessments and monitoring are carried out for each relevant area, as well as system-wide risks and that appropriate controls are in place for the identified risks.

The Coordinator will ensure adequate and routine training and education is available and is provided to all employees with access to customer information.

The Coordinator will, in consultation with other College offices, verify that existing policies, procedures and guidelines that provide for the security of customer information are adequate and routinely reviewed. The Coordinator shall make recommendation for revisions to and development of policies, procedures and guidelines, as appropriate.

The Coordinator will prepare an annual report on the effectiveness of the information security program. The report shall include current risk assessments performed for each relevant area, actions taken or to be taken to correct any security concerns identified, and any other information as required to provide assurance that this Information Security Program is implemented and maintained.

The Coordinator will maintain a consolidated "Information Policy and Procedure Manual" which includes this policy, each relevant area's documented procedures, and other regulatory information pertaining to the safeguarding of customer information.

(b) Identify and Assess Risks

The Information Security Program is intended to identify reasonable foreseeable external and internal risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control these risks.

Risk assessments will include a review of system-wide controls, testing, triggering events and monitoring activities, as well as risks unique to each relevant area with access to customer information.

Risk assessments at a minimum will include consideration of activities in each relevant area's operations, including:

(1) Employee awareness, training and management oversight.
(2) Information systems including network and software design, as well as information processing, storage, transmission, and disposal.
(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
(4) Preventative and detection controls

(c) Design and Routinely Test/Monitor Safeguards

Design and implement information safeguards to control the risks identified through risk assessment. The Coordinator will ensure the effectiveness of the safeguards' key controls, systems, and procedures are routinely tested and monitored.

Such safeguards, and their ongoing testing and monitoring will include the following:

(1) Employee Training and Management Oversight

Safeguards for security will include training of those individuals with authorized access to customer information. The College has adopted comprehensive policies, standards and guidelines for preserving the security of private information, including customer information.

The Coordinator will, working with relevant areas, identify categories of employees or others who have access to customer information. While each relevant area's manager is ultimately responsible for ensuring compliance with information security practices, the Coordinator will work in cooperation with each relevant area and Human Resources to develop training and education programs for all employees who have access to customer information. Training will include education on relevant policies and procedures and other safeguards in place or developed to protect customer information.

All college personnel will be required to take information security awareness training at least one time in an academic year.

Other safeguards will also be used, as appropriate, including job-specific training on maintaining security and confidentiality, requiring user-specific passwords and require passwords be based upon National Institute of Standards and Technology (NIST) guidelines, limiting access to customer information to those with a business need for access to information, requiring signed certification of responsibilities prior to authorizing access to systems containing customer information, requiring signed releases for disclosure of customer information, establishing methods for prompt reporting of loss or theft of customer information or media upon which customer information may be stored, and other measures that provide reasonable safeguards based upon the risks identified.

(2) Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to customer information.   This may include maintaining appropriate screening programs to detect attempts of unauthorized intrusions by means of hacking and viruses.

Safeguards for information processing, storage, transmission, retrieval and disposal may include, requiring electronic customer information be entered into a secure, password-protected system; using secure connections to transmit data outside the College network; using secure servers; encrypting transmitted customer information; ensuring customer information is not stored on transportable media (floppy drives, zip drives, etc.); permanently erasing customer information from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposal; storing physical records in a secure area and limiting access to that area; providing safeguards to protect customer information and systems from physical hazards such as fire or water damage; disposing of outdated records under a documented disposal policy; shredding confidential information before disposal; maintaining an inventory of servers or computers containing customer information; and other reasonable measures to secure customer information during its life cycle in the College's possession and control.

(3) Managing System Failures

The College will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software venders and others to regularly obtain and installing patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to customer information of threats to security; backing up data regularly and storing back up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

(4) Monitoring and Testing

Monitoring will be conducted to reasonably ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits, and any other reasonable measures adequate to verify that the information security program's controls, systems and procedures are working.

(d) Oversight of Service Providers

(1) The County College of Morris will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Require service providers by contract to implement and maintain such safeguards to protect customer information.

(e) Evaluation and Adjustment

The Coordinator will evaluate and adjust the information security program based on the results of ongoing monitoring and testing; any material changes to operations or business arrangements; or any other circumstances that are known or have reason to know that may have a material impact on protecting the privacy of customer information.