This Information Security Plan ("Plan") describes safeguards implemented by Northeast Community College to protect covered data and information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA). These safeguards are provided to:

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

This Information Security Program also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by Northeast Community College;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the program; and
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Policy Statement

GLBA mandates that the College appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Information Security Program Coordinator(s)

The Vice President of Financial Services and the Vice President of Technology Services (CIO) have been appointed as the coordinators of this Program at Northeast Community College. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information, and implementing procedures to minimize those risks to the Institute. Internal personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security policies and practices delineated in this program.

Identification and Assessment of Risks to Customer Information

Northeast Community College recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system

- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, the Northeast Community College Security team will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks.

Current safeguards implemented, monitored and maintained by the Northeast Community College Security team are reasonable, and in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the College. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Employee Management and Training

References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information (e.g. Student Accounts, Admissions Office, Financial Aid) are checked/performed. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information.

Physical Security

Northeast Community College has addressed the physical security of covered data and information by limiting access to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to Northeast Community College employees with an appropriate business need for such information. Furthermore, each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

Information Systems

Access to covered data and information via Northeast Community College computer information system is limited to those employees and faculty who have a legitimate business reason to access such information. The College has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security to Northeast Community College information systems. These policies and procedures, listed in Section 3 below, are available upon request from the Chief Information Security Officer.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, Northeast Community College has discontinued the use of social security numbers as student identifiers in favor of the College-Wide ID number as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

Management of System Failures

The Northeast Community College Security team has developed written plans and procedures to detect any actual or attempted attacks on Northeast Community College systems and has an Incident Response Plan which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This document is available upon request from the Chief Information Security Officer.

Oversight of Service Providers

GLBA requires the Institute to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program will ensure that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Security Program Coordinator(s) will identify service providers who have or will have access to covered data, and will work with the College Legal counsel and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data.

Continuing Evaluation and Adjustment

This Information Security Program will be subject to periodic review and adjustment, at least annually. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Program Coordinator(s), who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate. The Information Security Program Coordinator(s), in consultation with the Office of Legal Affairs, will review the standards set forth in this program 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/or internal or external threats to information security.

Policy Terms

Covered data and information - for the purpose of this program includes student financial information (defined below) that is protected under the GLBA. In addition to this coverage, which is required under federal law, Northeast Community College chooses as a matter of policy to include in this definition any and all sensitive data, including credit card information and checking/banking account information received in the course of business by the Institute, whether or not such information is covered by GLBA. Covered data and information includes both paper and electronic records.

Pretext calling - occurs when an individual attempts to improperly obtain personal information of Northeast Community College customers so as to be able to commit identity theft. It is accomplished by contacting the College, posing as a customer or someone authorized to have the customer's information,

and through the use of trickery and deceit (sometimes referred to as social engineering), convincing an employee of the Institute to release customer-identifying information.

Student financial information - is that information that Northeast Community College has obtained from a student or customer in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Related Procedures, Protocols, and Standards

Northeast Community College has adopted comprehensive policies, standards, and guidelines relating to information security, which are incorporated by reference into this Information Security Program. They include:

Procedures

- Information Security Administrative Procedure
- Privacy and Release of Information
- Identity Theft Prevention
- Acceptable Use – Technology Resources

Protocols

- Credit Card Processing Protocol
- InfoSec Incident Response Plan
- Security Awareness Plan

Standards

- Northeast Data Classification Standard
- Identity Verification Guidelines

Communication

Upon approval, this program shall be published on the Northeast Community College website. The following offices and individuals shall be notified via email and/or in writing upon approval of the program and upon any subsequent revisions or amendments made to the original document:

- Vice Presidents
- Director of Financial Aid
- Legal Counsel
- Technology Security team