WESTERN NEBRASKA COMMUNITY COLLEGE

President's Procedure

TITLE:	Gramm-Leach-Bliley Student Financial Information Security Program
DIVISION:	Educational Services
CATEGORY:	Information Technology
REFERENCE:	BP-810 Gramm-Leach-Bliley Student Financial Information Security Program Policy
NUMBER:	PP-810
DATE OF REVIEW:	
APPROVAL:	President's Cabinet

Purpose
Western Nebraska Community College (WNCC) recognizes the importance of complying with the Gramm-Leach-Bliley Act ("GLB"), a federal law that requires the College to implement and maintain a GLB Student Financial Information Security Program to safeguard student financial information.

Scope
This procedure applies to all WNCC employees who have access to student financial information or manage vendors who access student financial information.

Definitions
"Student financial information" means any customer data as defined in the GLB Act and includes any record containing nonpublic personally identifiable financial information about a student when offering a financial product or service to the student. 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, or other personally identifiable information or sensitive student data, in both paper and electronic format.

"Security breach" means any unauthorized disclosure, misuse, alteration, destruction or other compromise of student financial information, such as unauthorized access.

Procedure
This GLB Student Financial Information Security Program implements reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of student financial information as defined in the GLB Act.

The Program is designed to ensure the security and confidentiality of certain student financial information, protect against any anticipated threats to the integrity of such information and protect against unwarranted, unlawful or unauthorized disclosure, misuse, alteration or compromise of such information.

Designation of GLB Student Financial Information Security Program Coordinators: The College President designates the Executive Vice President and Chief Academic Officer (EVP/CAO), Chief Information Officer (CIO), the Chief Financial Officer (CFO), and Chief Student Services Officer (CSSO), collectively referred to as the "GLB Coordinators", to coordinate the protection of student financial information. The College President designates the responsibility for complying with this Policy with respect to their particular departments. The GLB Coordinators will coordinate the protection of student financial information with the Financial Aid Director, Information Security Specialist, Accounting Services Director, IT Associate Director, Human Resources Executive Director, and Dean of Instruction and Workforce Development, to implement the GLB Act requirements in this procedure. They will work together to identify reasonable and foreseeable internal and external risks to the security, confidentiality, and integrity of student financial information; to evaluate the effectiveness of the current safeguards for controlling these risks; to design and implement a safeguards program; and to regularly monitor and test the program. The GLB Coordinators will evaluate the program periodically to make appropriate adjustments and send reminders to the various college departments.

Risk Assessment and Safeguards: The GLB Coordinators will identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of student financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

The GLB Coordinators will work with all relevant areas of the College to identify potential and actual risks to security and privacy of the IT systems that contain student financial information.

The GLB Coordinators will assure that WNCC has procedures concerning the physical security of all central systems that contain or have access to student financial information and the network that is utilized to access the systems and will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, document retention policies and other procedures that may expose the College to risks.

The GLB Coordinators will develop written plans and procedures to detect any actual or attempted attacks on covered systems and have developed incident response procedures for actual or attempted unauthorized access to student financial information.

The GLB Coordinators will periodically review the disaster recovery program for critical systems.

Employee Training: The GLB Coordinators will develop training and education programs on GLB and this Program for all employees who have access to student financial information. Employees are required to participate in information security program training to include acceptable use and privacy procedures that govern confidential data, passwords and other information security guidelines.

Oversight of Service Providers and Contracts: GLB requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for student financial information. The College has developed contract language to ensure that all contracts that involve student financial information include a GLB privacy clause in compliance with GLB.

Evaluation and Revision of the Information Security Program: GLB mandates that this Student Financial Information Security Program be subject to periodic review and adjustment. Processes such as data access procedures and the training program will undergo regular review by the GLB Coordinators.

Notice of Security Breach: The Financial Aid Officer shall notify the GLB Coordinators and the U.S. Department of Education of any security breach of student financial information pursuant to the requirements of the Federal Student Aid Program Participation Agreement and the Student Aid Internet Gateway Agreement. Actual and suspected data breaches must be reported to the U.S. Department of Education on the day a data breach is detected or suspected. For guidance on reporting, please refer to the "Security Incident Reporting Form" attached to this Procedure. The Family Educational Rights and Privacy Act ("FERPA") and the Fair and Accurate Credit Transaction Act ("FACTA") may also apply to the confidentiality of student information. The President and the Board of Governors will be notified of a confirmed security breach of student financial information.

Revising this Procedure

This President's Procedure supersedes any prior WNCC policy, procedure, guideline or handbook on this subject matter.

WNCC reserves the right to revise this procedure, as necessary, or as new laws require attention.

Western Nebraska Community College

Security Incident Reporting Form

This form is to be used to report a detected or suspected security breach of student financial information, or unauthorized release of student personally identifiable information to the College Security Program Coordinator(s), as well as the U.S. Department of Education.

Intake Information

Date of Detected or Suspected Incident:

_____

Brief Description of Incident:

_____

_____

_____

Check all that apply:

_____Actual Breach

_____Suspected Breach

_____Student Financial Information

_____Student Personally Identifiable Information

_____Breach information can be linked to other PII without a password

_____Other, _____

Person Filing Incident Report:

_____

Name and Title

_____

Contact Information, email and phone number

_____

Internal Reporting

Please submit the Security Incident Reporting Form to any GLB Coordinator:

- Executive Vice President/Chief Academic Officer
- Chief Information Officer
- Chief Student Services Officer
- Chief Financial Officer

External Reporting

Report the Security Incident to any GLB Coordinator as noted above before reporting to the U.S. Department of Education. For reporting to the U.S. Department of Education, please submit an email to cpssaig@ed.gv to include the following information:

- Date of detected or suspected breach
- Impact of the breach
- Method of breach
- Include College Point of Contact
- Remediation status
- Next steps if needed

GLB requires the U.S. Department of Education be notified on the same day a Security Incident is detected.