Nebraska Wesleyan University's
GLBA Required Information Security Program

(Draft May 21, 2003)

I. Purpose

In order to continue to protect private information and data, and to comply with new federal law mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act **("GLBA")** effective May 23, 2003, Nebraska Wesleyan University has adopted this Information Security Program for certain highly critical and private financial and related information. This document describes the Information Security Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. This security program applies to customer financial information (**"covered data"**) the college receives in the course of business as required by these new federal laws, as well as other confidential financial information the college has voluntarily chosen as a matter of policy to include within its scope. The security program incorporates by reference the Institution's policies and procedures enumerated below and are in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

II. Definitions

"Covered data" means all information required to be protected under the Gramm-Leach-Bliley Act ("GLB Act"). "**Covered data**" also refers to financial information that the University, as a matter of policy, has included within the scope of this Information Security Program. **Covered data** shall mean any information: (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. "**Covered data**" consists of both paper and electronic records that are handled by the University or its affiliates.

"**Service Providers"** refers to all third parties who, in the ordinary course of college business, are provided access to **covered data**. Service providers may include businesses retained to transport and dispose of **covered data**, collection agencies, and systems support providers, for example.

III. Security Program Components

The GLB Act requires the college to develop, implement and maintain a comprehensive information security program containing the administrative, technical and physical safeguards that are appropriate based upon the institution's size, complexity and the nature of its activities. This Information Security Program has four components: (1) designating an employee or office responsible for coordinating the program; (2) conducting risk assessments to identify reasonably

foreseeable security and privacy risks; (3) ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored; and (4) overseeing service providers.

IV. Designation of Security Program Coordinators

The Security Program Coordinators will be responsible for implementing, coordinating and overseeing the Information Security Program. The Coordinators are presently the Controller and the Director of Information Technology. The Program Coordinators may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Coordinators or their designees.

The Coordinators will consult with responsible offices to identify units and areas of the colleges with access to **covered data**. As part of this Information Security Program, the Coordinators have identified units and areas of the institution with access to **covered data**. The Coordinators will confirm that all areas with covered information are included within the scope of this program.

The Coordinators will work with responsible parties to ensure adequate training and education is developed and delivered for all employees with access to **covered data**. The Coordinators will, in consultation with other college offices, verify that existing policies, standards and guidelines that provide for the security of **covered data** are reviewed and adequate. The Coordinators will make recommendations for revisions to policy, or the development of new policy, as appropriate.

The Coordinators will update this Information Security Program, including this and related documents, from time to time.

V. Risk Assessment

The Information Security Program will identify reasonably foreseeable external and internal risks to the security and confidentiality of **covered data** 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 consideration of risks in each area that has access to covered information. Risk assessments will include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures.

The Coordinators will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks, as well as risks unique to each area with **covered data**. The Coordinators will ensure that risk assessments are conducted on a regular basis, and more frequently where required. The Coordinators may identify a responsible party in each unit with access to **covered data** to conduct the risk assessment considering the factors set forth above, or employ other reasonable means to identify risks to the security, confidentiality and integrity of **covered data** in each area of the college with **covered data**.

VI. Information Safeguard and Monitoring

The risk assessment and analysis described above shall apply to all methods of handling or disposing of "**covered data**", whether in electronic, paper or other form. The Coordinators will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures**.**

VII. Service Providers

In the course of business, the college may from time to time appropriately share **covered data** with third parties. Such activities may include collection activities, transmission of documents, destruction of documents or equipment, or other similar services. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

The Coordinators will identify service providers who are provided access to **covered data**. The Coordinators will work with other offices as appropriate, to make certain that service provider contracts contain appropriate terms to protect the security of **covered data**.

VIII. Policies and Statements

The college has adopted comprehensive policies and statements relating to information security. They are incorporated by reference into this Information Security Plan, and include:

Policies:

Record Retention Policy
Computer Appropriate Use Account Policy
Electronic Mail Privacy Policy
World Wide Web Publishing Policy
Copyright Compliance Policy
Computer Privacy

Statements:

Computer Ethics and Policies Statement
Anti-Virus Standard (in process)
Employee Confidentiality Statement