Executive Memorandum No. 26

University of Nebraska Information Security Plan – Gramm Leach Bliley Compliance (effective May 23, 2003)

General Provisions

This Information Security Plan ("Plan") describes the University of Nebraska's safeguards to protect covered data and information. These safeguards are provided to:

1. Ensure the security and confidentiality of covered data and information;

2. Protect against anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to the individual to whom the information pertains.

This Plan also provides for mechanisms to:

1. Identify and assess the risks that may threaten covered data and information maintained by the University;

2. Develop written policies and procedures to manage and control these risks;

3. Implement and review the Plan; and

4. Adjust the Plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Covered Data and Information

In this Plan, the term "covered data and information" is defined as and includes Student Financial Information (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records. "Student Financial Information" is that information that the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University 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 as defined in 12 C.F.R. § 225.28. 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.

Identification and Assessment of Risks to Customer Information

The University recognizes that it has both internal and external risks. These risks include, but are not limited to:

1. Unauthorized access of covered data and information by someone other than the owner of the covered data and information

2. Compromised system security as a result of system access by an unauthorized person

3. Interception of data during transmission

4. Loss of data integrity

5. Physical loss of data in a disaster

6. Errors introduced into the system

7. Corruption of data or systems

8. Unauthorized access of covered data and information by employees

9. Unauthorized requests for covered data and information

10. Unauthorized access through hard copy files or reports

11. Unauthorized transfer of covered data and information through third parties

The University recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Department of the University of Nebraska Computing Services Network ("UNCSN") will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

Information Security Plan Coordinators

The Director of Networking of UNCSN is appointed as the coordinator of this Plan. At the time of the adoption of this Plan, the Director of Networking is Rick Golden (rgolden@nebraska.edu; 402.472.7626). In addition, each campus shall appoint a Campus Plan Coordinator to join with the Director of Networking to provide support in carrying out this Plan throughout the University. These five individuals will determine which University areas, departments and persons have access to covered data and information and will assess whether controls are in place to verify that these University areas, departments and persons comply with the requirements of this Plan. Further, 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 University.

At the time of the adoption of this Policy, UNCSN is engaged in planning, which includes the likelihood of hiring an individual for a newly created position with the title of Security Coordinator, or a similar title. Should such a position be created and filled, the University's Chief Information Officer may assign the duties set out in this Policy and presently assigned to the Director of Networking to the new position.

Design and Implementation of Safeguards Program

Employee Management and Training

Important information concerning the use of University information systems can be found in Presidential Executive Memorandum No. 16, Responsible Use of Computers and Information Systems, which discusses authorized access and other activities considered to be misuse of the University information system. Employees should be made aware of the existence and contents of Executive Memorandum No. 16, which is incorporated into this Plan by reference. Executive Memorandum No. 16 may be found at www.nebraska.edu. A serious and concerted effort shall be made to inform students and employees of the existence and contents of this Plan, using such means as are appropriate to educate the University community about this matter.

References of new employees working in areas that regularly work with covered data and information (e.g. Bursar's Office, Registrar, Financial Aid, Human Resources, Libraries, Payroll) shall be checked with particular attention paid to any information that may reflect upon the employees ability and aptitude to treat covered data and information confidential in accordance with the law and University policy. During employee orientation, each new employee in those departments identified as regularly working with covered data and information will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee shall receive training in the proper use of computer information systems and passwords. Training shall include controls and procedures to prevent employees from providing confidential information to unauthorized individuals and how to properly dispose of documents that contain covered data and information.

Each department responsible for maintaining covered data and information shall take serious and meaningful steps to protect information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data and information will regularly contact its campus Department of Human Resources to arrange for additional training on information privacy appropriate to the department. These training efforts should aim to minimize risk and safeguard covered data and information.

Information Systems

Access to covered data and information via the University's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to University employees in appropriate departments and positions.

The University will take reasonable and appropriate steps consistent with current technological developments to provide for the security, safety and integrity of all covered data and information of records in storage and transmission. UNCSN requires that all servers must be registered before being allowed through the University's firewall, thereby allowing UNCSN to verify that the system meets necessary security requirements as deemed appropriate by UNCSN practices and policies. These requirements include maintaining the operating system and applications, along with the application of appropriate patches and updates, in a timely fashion. Each campus and UNCSN will implement a written Password Policy for user and system passwords, designed to provide meaningful security within the system parameters and needs of each campus and Central Administration. In addition, an intrusion detection system shall be implemented to detect and stop certain external threats. An Incident Response Policy for occasions where intrusions do occur shall be implemented on each campus and at UNCSN.

When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information will be maintained on servers that are behind the University's firewall.

All firewall software and hardware maintained by UNCSN will be kept current. UNCSN will continue to develop and implement policies and procedures to provide security to the University's information systems. Further, UNCSN will provide campuses with coordination and support to develop and implement similar policies. These policies shall be distributed to the University community and other information providers through posting on University websites and other means deemed appropriate.

The University will not use Social Security Numbers to identify students, employees, or other information providers, outside of those identification uses specifically required by law, such as in financial aid, payroll and benefit functions.

Management of System Failures

UNCSN and each campus shall without undue delay develop written plans and procedures to detect any actual or attempted attacks on University systems, along with an Incident Response Policy which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This policy shall be distributed to the University community and other information providers through posting on University websites and other means deemed appropriate.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the University determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. Contracts with service providers may include the following provisions:

1. An explicit acknowledgment that the contract allows the service provider access to confidential information;

2. A specific definition or description of the confidential information being provided;

3. A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

4. An assurance from the service provider that it will protect the confidential information it receives from the University according to commercially acceptable standards and no less rigorously than it protects its own confidential information;

5. A provision providing for the return or destruction of all confidential information received by the service provider upon completion or termination of the contract;

6. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the University to terminate the contract without penalty; and

7. A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Attached to this Plan is a model contract provision for Service Providers. Contracts entered into prior to June 24, 2002, are grandfathered for purposes of compliance with GLB until May 24, 2004. All existing contracts entered into on or after June 24, 2002, and all future contracts should contain provisions substantially similar to the attachment.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within UNCSN, where constantly changing technology and evolving risks mandate increased vigilance. Similar reviews shall be directed by the Campus Plan Coordinators on their respective campuses. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the five Plan Coordinators who will assign specific responsibility for implementation and administration as appropriate. The Plan Coordinators will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the Plan to reflect changes in technology, the sensitivity of covered data and information, and internal or external threats to information security.

Reference: June 24, 2003

UNIVERSITY OF NEBRASKA
CONFIDENTIAL INFORMATION
GLB ACT ADDENDUM

This Addendum ("Addendum") amends and is hereby incorporated into the existing agreement known as _____ ("Agreement"), entered into by and between _____ (hereinafter "Service Provider") and the Board of Regents of the University of Nebraska on behalf of _____ (the "University").

The University and Service Provider mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Gramm Leach Bliley Act ("GLB") dealing with the confidentiality of customer information and the Safeguards Rule. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

1. Definitions:

   a. Covered Data and Information includes Student Financial Information (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

   b. Student Financial Information is that information that the university has obtained from a student in the process of offering a financial product or service, or such information provided to the University 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 as defined in 12 C.F.R. § 225.28. 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.

2. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information. Specifically, access to the following categories of Covered Data and Information is anticipated under the Agreement:

   _____

   _____

3. Prohibition on Unauthorized Use of Disclosure of Covered Data and Information: Service Provider agrees to hold the Covered Data and Information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of the University except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by the University.

4. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of the University according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

5. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:

a. Return to the University or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of the University. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of Covered Data and Information. Service Provider shall complete such return or destruction as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of the Agreement. Within such thirty (30) day period, Service Provider shall certify in writing to the University that such return or destruction has been completed.

b. If Service Provider believes that the return or destruction of Covered Data and Information is not feasible, Service Provider shall provide the protections of this Addendum to Covered Data and Information received from or created on behalf of the University, and limit further uses and disclosures of such Covered Data and Information, for so long as Service Provider maintains the Covered Data and Information.

6. Term and Termination:

a. This Addendum shall take effect upon the earlier of execution or May 23, 2003.

b. In addition to the rights of the parties established by the underlying Agreement, if the University reasonably determines in good faith that Service Provider has materially breached any of its obligations under this Addendum, the University, in its sole discretion, shall have the right to:

(i) exercise any of its rights to reports, access and inspection under this Addendum; and/or

(ii) require Service Provider to submit to a plan of monitoring and reporting, as the University may determine necessary to maintain compliance with this Addendum; and/or

(iii) provide Service Provider with a fifteen (15) day period to cure the breach; and/or

(iv) terminate the Agreement immediately if Service Provider has breached a material term of this Addendum and cure is not possible.

c. Before exercising any of these options, the University shall provide written notice to Service Provider describing the violation and the action it intends to take.

7. Subcontractors and Agents: If Service Provider provides any Covered Data and Information which was received from, or created for, the University to a subcontractor or agent, then Service Provider shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Provider by this Addendum.

8. Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, the University.

9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Provider shall report to the University any use or disclosure of Covered Data and Information not

authorized by this Addendum or otherwise authorized in writing by the University. Service Provider shall make the report to the University not less than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Covered Data and Information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Service Provider had done or shall do to mitigate any deleterious effect of unauthorized use or disclosure, and (v) what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure. Service Provider shall provide such other information, including a written report, as reasonably requested by the University.

10. Indemnity. Service Provider shall defend and hold the University harmless from all claims, liabilities, damages, or judgments involving a third party, including the University's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Addendum.

11. Survival. The respective rights and obligations of Service Provider under Section 5 shall survive the termination of this Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

The Board of Regents of the University of Nebraska	SERVICE PROVIDER:_____ Print name
By:_____	By:_____
Title:_____	Title:_____
Date:_____	Date:_____