UNL Animal Science Department

Data and System Security Classification

Executive Memorandum No. 16

Executive Memorandum No. 26

University of Nebraska Lincoln General Privacy Policy

In compliance to the University Standards
I. Data Classification – Animal Science Data that is owned and maintained by Animal Science personnel shall be put into appropriate classification levels according to their sensitivity and criticality.

A. Unrestricted data – Data in this Classification is for public viewing and use. There are no restrictions, no distribution limitations and is open to the public.

This is data that is distributed like brochures, news releases, formal statements, newsletters, annual reports, web pages, bulletin boards, twitter, Facebook etc.

This data is freely given or shown for any and all to see, receive, or pick-up.

The only security threat for this information is unauthorized or unintentional alterations, distortion, or destruction of the data.

The security for this data is on the equipment that houses it. Animal Science uses the University housed server for website, brochures, etc. and all are behind password protected firewalls.

Examples of this type of data include but are not limited to:

1. Website
2. Brochures
3. Animal Science Newsletter
4. Block and Bridal Annual
5. News Releases

B. Sensitive – Data in this classification is information retained in the University Employment data base, information gathered about any employee of the Animal Science Department, all release forms signed by employees, any data in this classification is confidential and only those persons with explicit need for this data will have access to it. Password protected authorization is needed to access this information.

It is housed in the main University of Nebraska database in a secure server maintained by the University of Nebraska Lincoln.

Examples of this data are:

1. Employment
2. Training data
3. Occupational Licenses,
1. Job Description
4. Job Title
5. Personal information like Address, Phone

C. Very sensitive – The data in this classification is the data that is restricted by federal statutes and regulations and are forms of private information. This information is housed in the University of Nebraska Database and is on a secure server. This data is only accessed by those persons with password protected authority to access this information. It is never put out in public, never given out to anyone except the person the information is about. No one is to use the data in any matter not explicitly documented in the privacy policy written by the University of Nebraska administration department.

This information is privacy intensive and is not readily available to anyone except those persons that have been authorized by the University of Nebraska to access this information.

This information can only be changed with a written request by the person who the information is about.

Security threats to this data include violation of privacy statutes and regulations in addition to unauthorized alterations or destruction. If this date were accessed by unauthorized persons, it could cause financial loss or allow identity theft.

Examples:
1. Social Security Numbers
2. Most home addresses
3. Educational records and Grading systems such as Blackboard
4. Health and medical data
5. Library borrower’s records
6. Signature Imaging data
7. Criminal history data
8. Drivers License Numbers
9. Personal biometric data (fingerprint, voice print, retina or iris image, or other unique physical representation)

10. Financial account number including credit or debit cards when stored in combination with a PIN or security code

11. Unique electronic identification number or routing code in combination with required security code, access code or password

Security practices are to limit storage of this data to only those instances where the department is required to retain it by federal or state law, and to limit access to the data to campus only IP addresses and only to those staff who are required to handle the data. Retention Policy - Departments are expected to follow those policies as they pertain to the data being stored. All sensitive data being stored on campus must meet a variety of security best practices.

D. Extremely sensitive – Data in this classification is data whose disclosure or corruption could be hazardous to life or health.

This data is the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health or safety repercussions. Very strict rules must be adhered to in the usage of this data.

Examples:

1. Contents of law enforcement investigative records and communications systems
2. Designated Research Projects (such as finding cures for diseases, poisons, or biohazard material usage etc.)
Executive Memorandum No. 16

Policy for Responsible Use of University Computers and Information Systems

1. Purpose

   It is the purpose of this Executive Memorandum to set forth the University's administrative policy and provide guidance relating to responsible use of the University's electronic information systems.

2. General

   The University of Nebraska strives to maintain access for its faculty, staff, students, administrators and Regents (the "users") to local, national and international sources of information and to provide an atmosphere that encourages sharing of knowledge, the creative process and collaborative efforts within the University's educational, research and public service missions. Access to electronic information systems at the University of Nebraska is a privilege, not a right, and must be treated as such by all users of these systems. All users must act honestly and responsibly. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements related to University information systems. All users shall act in accordance with these responsibilities, and the relevant local, state and federal laws and regulations. Failure to so conduct oneself in compliance with this Policy may result in denial of access to University information systems or other disciplinary action.

   The University of Nebraska is a provider of a means to access the vast and growing amount of information available through electronic information resources. The University of Nebraska is not a regulator of the content of that information and takes no responsibility for the content of information, except for that information the University itself and those acting on its behalf create. Any persons accessing information through the University of Nebraska information systems must determine for themselves and their charges whether any source is appropriate for viewing.

   Accepting any account and/or using the University of Nebraska’s information systems shall constitute an agreement on behalf of the user or other individual accessing such information systems to abide and be bound by the provisions of this Policy. The University may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of University policies or state or federal laws. When it has been determined that there has been a violation, the University may restrict or prohibit access by an offending party to its information systems through University-owned or other computers, remove or limit access to material posted on University-owned computers or networks, and, if warranted, institute other disciplinary action.

3. Definitions

   For purposes of this policy the following definitions shall apply:
   
   a. **Electronic communications** shall mean and include the use of information systems in the communicating or posting of information or material by way of electronic mail, bulletin boards,
World Wide Web (internet), or other such electronic tools.

b. **Information systems** shall mean and include computers, networks, servers and other similar devices that are administered by the University and for which the University is responsible. "Networks" shall mean and include video, voice and data networks, routers and storage devices.

c. **Obscene** with respect to obscene material shall mean (1) that an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion, (2) the material depicts or describes in a patently offensive way sexual conduct specifically set out in Neb. Rev. Stat. §§ 28-807 to 28-809, as amended, and (3) the material taken as a whole lacks serious literary, artistic, political, or scientific value.

4. **Permitted Uses**

a. **University Business Use and Limited Personal Use.**

   University information systems are to be used predominately for University-related business. However, personal use is permitted so long as it conforms with this Policy and does not interfere with University operations or an employee user's performance of duties as a University employee. As with permitted personal use of telephones for local calls, limited personal use of information systems does not ordinarily result in additional costs to the University and may actually result in increased efficiencies. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material is prohibited. UNDER ALL CIRCUMSTANCES, PERSONAL USE BY EMPLOYEES MUST COMPLY WITH SUBSECTION b. OF THIS SECTION AND SHALL NOT CONFLICT WITH AN EMPLOYEE'S PERFORMANCE OF DUTIES AND RESPONSIBILITIES FOR THE UNIVERSITY. Personal use may be denied when such use requires an inordinate amount of information systems resources (e.g. storage capacity).

b. **Prior Approval Required for Personal Use for Outside Consulting, Business or Employment.**

   Personal use of University information systems resources or equipment by any user for personal financial gain in connection with outside (non-University) consulting, business or employment is prohibited, except as authorized for employees by Section 3.4.5 of the Bylaws of the Board of Regents. Employee personal use in conjunction with outside professional consulting, business or employment activities is permitted only when such use has been expressly authorized and approved by the University Administration or the Board of Regents, as appropriate, in accordance with the requirements of said Section 3.4.5 of the Bylaws.

5. **Access**

   Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relation with the University of Nebraska, his or her ID and password shall be denied further access to University computing resources.


   Misuse of University information systems is prohibited. Misuse includes the following:

   a. Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.
b. Accessing without proper authorization computers, software, information or networks to which
the University belongs, regardless of whether the resource accessed is owned by the University or
the abuse takes place from a non-University site.

c. Taking actions, without authorization, which interfere with the access of others to information
systems.

d. Circumventing logon or other security measures.

e. Using information systems for any illegal or unauthorized purpose.

f. Personal use of information systems or electronic communications for non-University consulting,
business or employment, except as expressly authorized pursuant to Section 3.4.5 of the Bylaws
of the Board of Regents.

g. Sending any fraudulent electronic communication.

h. Violating any software license or copyright, including copying or redistributing copyrighted
software, without the written authorization of the software owner.

i. Using electronic communications to violate the property rights of authors and copyright owners.
(Be especially aware of potential copyright infringement through the use of e-mail. See the
provisions under "E-Mail" contained in this Policy.)

j. Using electronic communications to harass or threaten users in such a way as to create an
atmosphere which unreasonably interferes with the education or the employment experience.
Similarly, electronic communications shall not be used to harass or threaten other information
recipients, in addition to University users.

k. Using electronic communications to disclose proprietary information without the explicit
permission of the owner.

l. Reading other users' information or files without permission.

m. Academic dishonesty.

n. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University
records (including computerized records, permits, identification cards, or other documents or
property).

o. Using electronic communications to hoard, damage, or otherwise interfere with academic
resources available electronically.

p. Using electronic communications to steal another individual's works, or otherwise misrepresent
one's own work.

q. Using electronic communications to fabricate research data.

r. Launching a computer worm, computer virus or other rogue program.

s. Downloading or posting illegal, proprietary or damaging material to a University computer.

t. Transporting illegal, proprietary or damaging material across a University network.
u. Personal use of any University information system to access, download, print, store, forward, 
transmit or distribute obscene material.

v. Violating any state or federal law or regulation in connection with use of any information system.

7. Privacy

a. User Privacy Not Guaranteed. When University information systems are functioning properly, a 
user can expect the files and data he or she generates to be private information, unless the creator 
of the file or data takes action to reveal it to others. Users should be aware, however, that no 
information system is completely secure. Persons both within and outside of the University may 
find ways to access files. ACCORDINGLY, THE UNIVERSITY CANNOT AND DOES NOT 
GUARANTEE USER PRIVACY and users should be continuously aware of this fact.

b. Repair and Maintenance of Equipment. Users should be aware that on occasion duly authorized 
University information systems technological personnel have authority to access individual user 
files or data in the process of performing repair or maintenance of computing equipment the 
University deems is reasonably necessary, including the testing of systems in order to ensure 
adequate storage capacity and performance for University needs. Information systems 
technological personnel performing repair or maintenance of computing equipment are prohibited 
by law from exceeding their authority of access for repair and maintenance purposes or from 
making any use of individual user files or data for any purpose other than repair or maintenance 
services performed by them.

c. Response to a Public Records Request, Administrative or Judicial Order or Request for Discovery 
in the Course of Litigation. Users should be aware that the Nebraska public records statutes are 
very broad in their application. Certain records, such as unpublished research in progress, 
proprietary information, personal information in personnel and student records are protected from 
disclosure. However, most other University records contained in electronic form require 
disclosure if a public record request is made. Users should remember this when creating any 
electronic information, especially e-mail. Also, users should be aware that the University will 
comply with any lawful administrative or judicial order requiring the production of electronic 
files or data stored in the University's information systems, and will provide information in 
electronic files or data stored in the University's information systems in response to legitimate 
requests for discovery of evidence in litigation in which the University is involved.

d. Response to Misuse of Computers and Network Systems. When for reasonable cause, as such 
cause may be determined by the Office of the Vice President and General Counsel, it is believed 
that an act of misuse as defined in section 6 above has occurred, then the chief information 
services officer serving Central Administration or serving the relevant campus may access any 
account, file or other data controlled by the alleged violator and share such account information, 
file or other data with those persons authorized to investigate and implement sanctions in 
association with the misuse of the University's computer and information systems. Should any of 
the chief information service officers reasonably believe that a misuse is present or imminent 
such that the potential for damage to the system or the information stored within it, is genuine and 
serious (e.g. hacking, spamming or theft), then the chief information officer may take such action 
as is necessary to protect the information system and the information stored in it, including the 
denial of access to any University or non-University user, without a determination from the 
Office of the Vice President and General Counsel regarding reasonable cause; provided however, 
that the chief information officer shall contact the Office of the Vice President and General 
Counsel as soon as possible to confirm that any protective actions taken were appropriate and 
within the parameters of this executive memorandum.
e. Access to Information Concerning Business Operations. Employees regularly carry out the business functions of the University using the University's information systems. Business records, inquiries and correspondence are often stored such that individuals may control the access to particular information stored within the University's information system. Should any employee become unavailable, be incapacitated due to illness or other reasons, or refuse to provide the information necessary to carry out the employee's job responsibilities in a reasonably timely manner, then following consultation with and approval by the Office of the Vice President and General Counsel, the chief information officer of Central Administration or of the relevant campus may access the employee's records in order to carry out University business operations on behalf of the unavailable or uncooperative employee.

8. E-mail

a. Applicability. ALL POLICIES STATED HEREIN ARE APPLICABLE TO E-MAIL. E-mail should reflect careful, professional and courteous drafting—particularly since it is easily forwarded to others. Never assume that only the addressee will read your e-mail. Be careful about attachments and broad publication messages. Copyright laws and license agreements also apply to e-mail.

b. E-mail Retention. E-mail messages should be deleted once the information contained in them is no longer useful. When e-mail communications are sent, the e-mail information is stored in one or more backup files for the purposes of "disaster recovery", i.e. inadvertent or mistaken deletions, system failures. In order to provide for the recovery of deleted e-mail, while maintaining efficient use of storage capabilities, e-mail information on backup files shall be retained for a period of time not to exceed seven days.

9. Web Pages

The Central Administration and each University campus may establish standards for those Web Pages considered to be "official" pages of the University. All official Web Pages shall contain the administrative unit's logo in the header and footer in order to identify it as an official University of Nebraska Web Page. No other Web Pages shall be allowed to use University of Nebraska logos without the express permission of the University. Originators of all Web Pages using information systems associated with the University shall comply with University policies and are responsible for complying with all federal, state and local laws and regulations, including copyright laws, obscenity laws, laws relating to libel, slander and defamation, and laws relating to piracy of software.

The persons creating a Web Page are responsible for the accuracy of the information contained in the Web Page. Content should be reviewed on a timely basis to assure continued accuracy. Web Pages should include a phone number or e-mail address of the person to whom questions/comments may be addressed, as well as the most recent revision date.

10. Notification

This Policy shall be published in all employee and faculty handbooks and student catalogs, and placed on the World Wide Web in order to fully notify users of its existence.

11. Application and Enforcement

This Policy applies to all administrative units of the University of Nebraska. The Central Administration and each University campus is encouraged to provide supplemental policy guidance, consistent with this Policy, designed to implement the provisions herein.
Each University campus shall be responsible for enforcing this Policy in a manner best suited to its own organization. It is expected that enforcement will require cooperation between such departments as computer systems administration, human resources, affirmative action, academic affairs and student affairs. Prior to any denial of access or other disciplinary action, a user shall be provided with such due process as may be recommended by the University's Office of the General Counsel.

Reference: August 28, 2001
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

This next page is an addendum that was added to the document and it was voted on and passed even though it has places to fill in information you can simply read it and do not sign it.
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:

---

Executive Memorandum No. 26
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: __________________________

This is a copy of the document that was signed by the University to make this addendum part of the Executive Memorandum No. 26. You do not have to sign this document.
University of Nebraska-Lincoln
General Privacy Policy
(As approved by the Faculty Senate – January 2003)

Our Commitment to You

The University of Nebraska-Lincoln will attempt to safeguard the privacy of all visitors to publicly accessible web sites (that is, web sites not password protected) to the extent allowed by law. This notice describes our privacy policy as it relates to the collection, protection, and disclosure of such information resulting from University web servers, including University web sites, sites that collect online information, or that identify actions of a web user.

Other privacy standards apply to such things as password-protected web sites, instructional web sites, student records and employee personnel records as specifically identified in State Statute, in accordance with federal or state laws and University policies and by-laws.

The University of Nebraska-Lincoln web pages may contain links to other sites on the World Wide Web; however, the University is not responsible for any content or services provided on these sites.

Voluntary Information Requested from You

Information provided on a volunteer basis, during routine requests for personal information (such as surveys, email addresses, requests for information, etc.) will be used only for the purpose(s) outlined. Every web page that requests information from you should disclose the purpose of how this information will be used. If you do not wish to have the information used in the manner listed, or if the potential use of the information is not outlined, you are not required to provide it, however, you may not receive certain services if the information is not provided.

Information We Collect Automatically

The information collected and logged through University web sites can be classified into two categories: web site logs and cookies.

Web Site Logs

The University of Nebraska-Lincoln makes no attempt to identify individual visitors from information collected in web site logs, except in cases where system integrity, institutional infrastructure, or personal safety is being jeopardized. The data is used to tune the web pages and the site for efficiency, to produce summary reports regarding system usage and give system administrators the ability to monitor system integrity, and protect institutional infrastructure and personal safety. The usage information gathered is also used to customize web sites (move high use pages to the top of the site, add content for information frequently searched for, establish patterns of interest, etc.).

Information collected and logged through University web sites and web servers includes the following:

- Internet addresses or URLs of computers used in browsing a web site
- Web pages requested
- The date and time of a visit to a web page
- The browser version and configuration information used to connect to a site
- Search terms used on our search engines

Cookies

There are university sites that require cookies. We neither forward cookies nor intentionally collect information for other parties outside UNL.

Sharing Information

We disclose any nonpublic information only when it is necessary for the conduct of University, State, or Federal government business, or under circumstances where disclosure is required by law. Information may also be disclosed for audit purposes, to regulatory agencies, or for other general administrative services. Information is not intentionally disclosed or distributed to any entity who uses it to sell products or services. Information will not be released without written authorization to the extent allowed by law.

Questions

If you have questions about the collection of information or concerns about adherence to this policy from University of Nebraska-Lincoln web sites, please contact the University Communications Office.

Effective Date of General Privacy Policy – 10/1/2002

December 2002