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:

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

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

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.

Design and Implementation of Safeguards Program

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

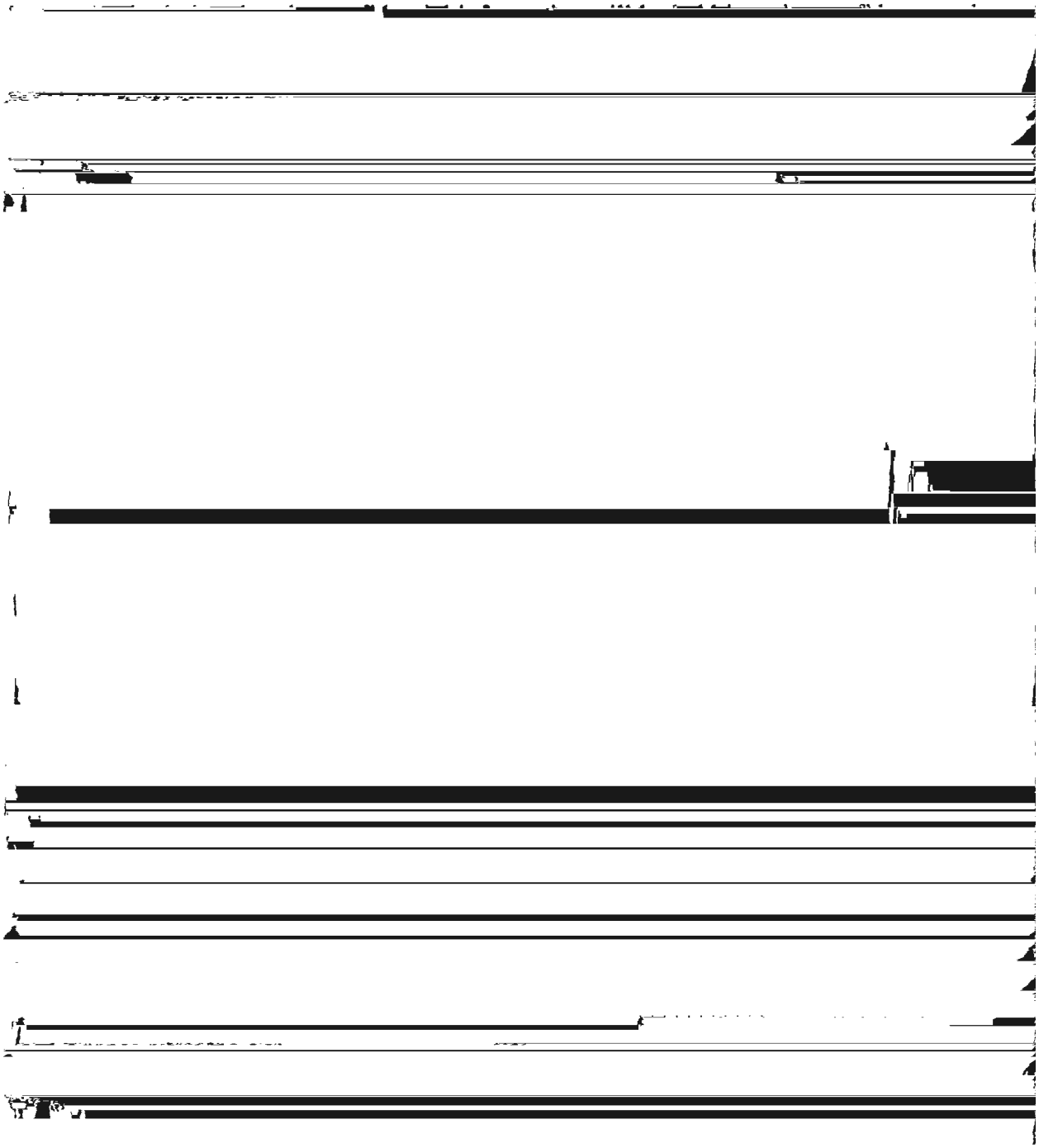
and information, including, but not limited to, accounts, balances, and transactional information, are available only to University employees in appropriate departments and

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;

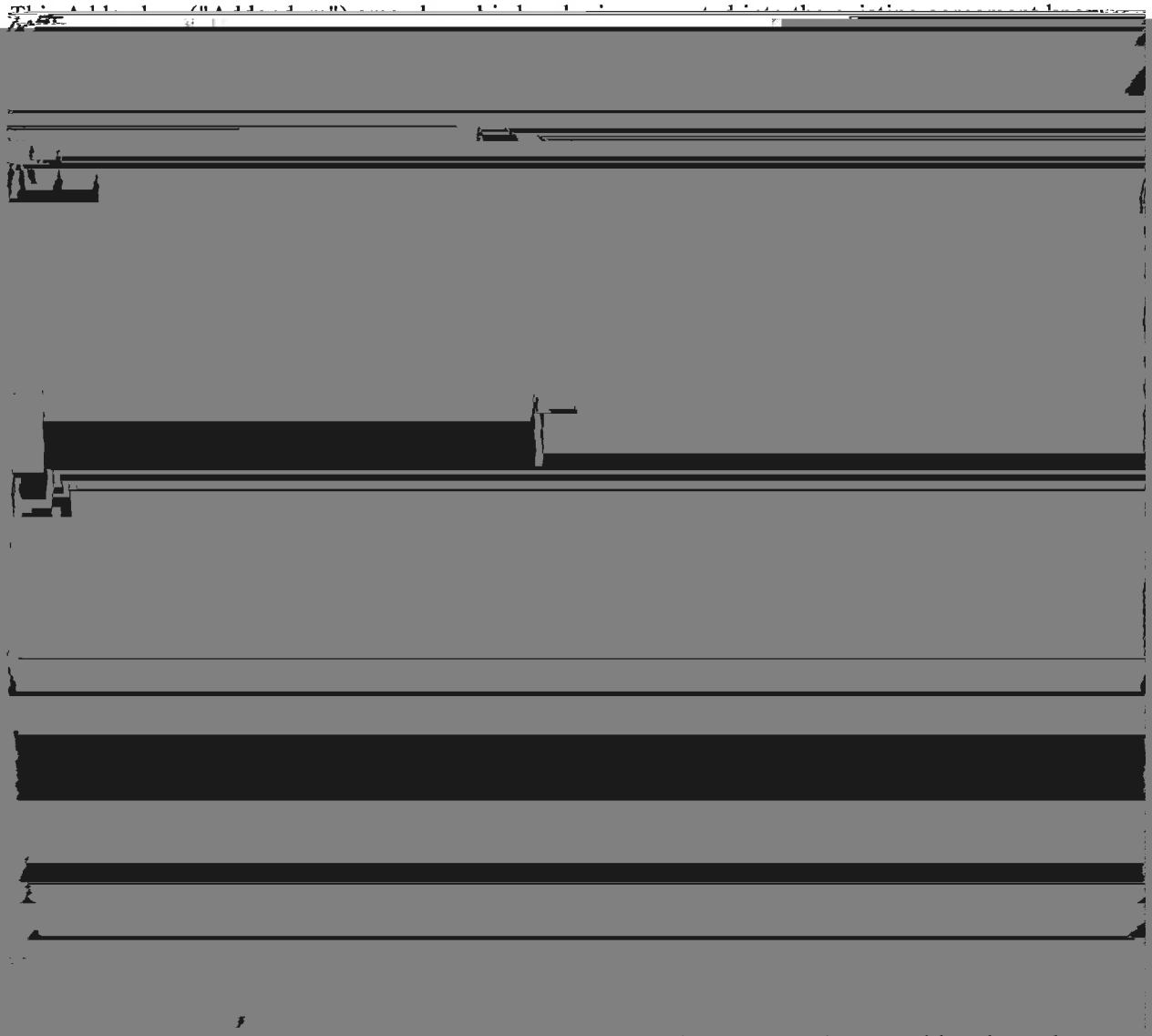
2 A specific definition or description of the confidential information being provided;



Reference: September 9, 2014

James , M.D.
In t
University of Nebraska

UNIVERSITY OF NEBRASKA
CONFIDENTIAL INFORMATION
GLB ACT ADDENDUM



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

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

[redacted]

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

[redacted]

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.