# Customer Information Safeguarding Program

## Introduction

The Gramm-Leach-Bliley (GLB) Act of 2000 requires financial institutions to ensure the security and confidentiality of customer information. Universities and colleges are deemed to comply with the privacy provision of the Act if they are in compliance with Family Educational Rights and Privacy Act (FERPA) of 1974; however, universities and colleges are still subject to the requirements of administrative, technical and physical safeguarding of customer information. The written safeguarding program outlined below will address the administrative, technical and physical safeguarding of customer information. The objectives of the safeguards are as follows:

- Ensure the security and confidentiality of customer information,
- Protect against any anticipated threats or hazards to the security or integrity of such information, and
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

## Definitions

- "Customer information" means any record containing nonpublic personal information as defined in 16 CFR 313.3(n) (Federal Register, Vol. 65, No. 101, Wed., May 24, 2000) about a customer of MSU, whether in paper, electronic or other form (16 CFR 314.2(b)).
- "Nonpublic personal information" is personally identifiable financial information and lists derived there from.
- "Customer" is an individual who obtains or has obtained a financial product or service from MSU that is to be used primarily for personal, family, or household purposes (16 CFR 313.3(e), (h)).

## Plan Responsibility, Review, Updates, and Approval

Responsibility for MSU's customer information security program is assigned to a customer information safeguarding team comprised of the following positions:

| **Area** | **Position** |
|---|---|
| Business Affairs | Vice President (Chair) |
| Student Affairs | Vice President |
| ITS | CIO |

This security plan will be reviewed and updated regularly by this team and approved annually by the President of MSU.

These positions will work together and be responsible for coordinating MSU's information security program, including the following:

- Identification of reasonably foreseeable internal/external risks to the security that could result in unauthorized disclosure, misuse of information;
- Design and implementation of the safeguard program;

- Regularly monitor and test the sufficiency of any safeguards in place to control risks in the following areas:
    - Employee Management & Training;
    - Information Systems; and
    - Managing System Failures.

**Identification, Assessment, Management & Control of Risks**

MSU recognizes that there are both internal and external risks at three different levels: 1) NDUS Core Technology Services (CTS), 2) MSU Information Technology Services (ITS) department, 3) other MSU department systems.

1. North Dakota University System Core Technology Services (CTS)

    a. The CTS is a cooperative effort among the eleven campuses of the North Dakota University System for the provisioning of enterprise-wide IT services.

    b. CTS obligations are addressed in North Dakota University System Policy Section 1912: Public Records and NDUS Procedure Section 1912.1: Information Security Procedures.

2. MSU Information Technology Services (ITS) department

    a. MSU ITS is responsible for providing a secure computing environment for the faculty, staff and students. This environment, for MSU, includes the campus infrastructure; the Local Area Network; file and application servers for research, academic and administrative functions.

    Potential risks associated with ITS systems include the following:

    - unauthorized access and/or use of personal customer information by means of computer and electronic data by external parties,
    - system failure.

    Physical access to networking equipment and administrative servers is controlled by lock and key, with only those people needing to maintain the infrastructure itself having access. Electronic access is controlled by passwords and access control lists. It should be noted that the responsibility for secure transmissions resides as much with the origin and destination of the transmission as it does with the medium facilitating that transmission.

    Access to the administrative file servers is authorized by the individual departments and granted by the system administrator for the servers. The storage area on the servers consists of individual and shared directories. The individual storage is password protected for the specific individual account. Access to the shared area for the department is authorized by the department and implemented by the system administrator.

    No passwords granting access to data are maintained in plain text. No passwords are altered for an individual or given to an individual until it has been determined that the individual is the person entitled to access the account.

    All incoming email is filtered for spam and scanned for viruses. File servers are scanned for viruses. Anti-virus software and spam filters are maintained at a current level.

File and application servers are backed up on a regular basis. The back-up library is maintained in a secondary secured facility on campus.

3. Other MSU department systems

This level consists of MSU administrative departments and employees that have access to administrative information that could include private customer information. Information in this category is obtained by MSU employees from CTS systems, ITS systems, or information systems maintained within the MSU administrative or academic department itself.

Potential risks in this category include the following:

- unauthorized access and/or use of personal customer information by means of computer and electronic data, or paper documents and files,
- lack of employee knowledge about the privacy of customer information,
- system failure.

Management and control responsibilities for MSU departmental information systems and employees actions rest with the department heads and the administrative chain of command shown in the MSU organizational chart. Management and control responsibilities fall under three general categories: A) Employee Management and Training, B) Information Systems, and C) Managing System Failures.

A) Employee Management and Training

The success or failure of any security plan largely depends on its employees. Because certain customer information (such as: social security numbers) is available to a large number of MSU employees via the administrative systems (ConnectND), risk of failure is slightly higher in this area. As a result of this risk, the following steps will be taken:

1. All departments are encouraged to check references prior to hiring employees.
2. Every employee with administrative computer system access to name and address information will be annually notified and reminded of MSU policy 1912.1 and the need to keep customer information confidential and properly safeguarded.
3. CTS administrative computer systems require the use of a strong password (at least eight characters long) and frequent password changes.
4. Employees will be reminded annually to take steps to maintain security and confidentiality of customer information, such as:

   -locking rooms and filing cabinets where records are stored;

   -locking desk drawers;

   -recognizing any fraudulent attempt to obtain customer information;

   -limit access to data in software programs.
5. MSU will limit access to customer information to employees who have a business purpose for access which in part will be accomplished through the administrative system (ConnectND) security access authorization form process. Department heads must sign the form granting access prior to being granted to an

employee. MSU Financial Processing Guidelines require the deletion or change of administrative system access for terminating or transferring employees.

6. Impose disciplinary measures for any employee breaches.

B) Information Systems

Information systems include network and software, information processing, storage, transmission, retrieval and disposal. Department heads will be notified annually of the following standards for information system security:

1. Store records in a secure area with access limited to authorized employees.
    a. Store paper records in a room or file cabinet that is locked when unattended.
    b. Ensure that storage areas are protected against potential destruction (fire etc.).
    c. Store electronic customer information on a secure server in which data is accessed with passwords and the server is in a secure area.
2. Provide secure data transmission.
    a. Collect sensitive financial data - Use Secure Sockets Layer (SSL) or encryption.
    b. If collecting information directly from the consumer. Caution the consumer about sending sensitive data via e-mail.
    c. If transmitting sensitive data via e-mail, use encryption.
3. Dispose of customer information in secure manner.
    a. Designate a record retention manager to dispose of nonpublic information.
    b. Shred all outdated customer information.
    c. When disposing of computers, erase all data on; diskettes, tapes, hard drives, etc.
4. Maintain an inventory of office computers.

C) Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions and system failures. Department heads will annually be notified of the following MSU standards for managing system failures:

1. Maintain up-to-date and appropriate programs.
    a. Check with software vendors regularly to obtain patches that resolve vulnerabilities.
    b. Use anti-virus software that updates automatically.
    c. Maintain up-to-date firewalls particularly if using broadband Internet access, or if employees are allowed to connect from home or off-site.
    d. Provide central management of security tools for employees and pass along updates about any security risks or breaches.

2. Takes steps to preserve security, confidentially and integrity of customer information. Backup customer information data regularly.
3. Notify customer promptly if nonpublic information (NPI) is subject to loss, damage or unauthorized access.
4. Maintain systems and procedures to ensure that access is limited to authorized employees.

**Oversight of Service Providers and Contracts**

GLB requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. MSU's Business Office in cooperation with the North Dakota Office of the Attorney General will develop and send form letters to all covered contractors requesting assurances of GLB compliance. The MSU Business Office, in consultation with the North Dakota Office of the Attorney General will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

**Approved: December 6, 2004**
**Reviewed: Fall, 2008**
**Revised: Summer, 2015**
**December, 2016**

**Sponsor: Vice President for Academic Affairs**