New Mexico State University

WRITTEN INFORMATION SECURITY PROGRAM

Version 3

August 2021

Chief Information Security Officer
Chief Privacy Officer and IT Compliance Office

Table of Contents

Revision History

Guidelines for NMSU Policy 15.63 (Protection of Customer Information; GLBA)Issued by NMSU ICT on 5/21/03; Non-Substantive edits 10/21/15; Substantive edits 07/26/21

Background

The Gramm-Leach-Bliley Act (GLBA), which was signed into law on November 12, 1999, created a requirement that financial institutions must have certain information privacy protections and safeguards in place. The Federal Trade Commission (FTC) has enforcement authority for the requirements and has determined that higher education institutions are financial institutions under GLBA.

Each institution, including New Mexico State University (NMSU), has agreed to comply with GLBA in its Program Participation Agreement with the U.S. Department of Education. In addition, as a condition of accessing the department's systems, each institution and servicer must sign the Student Aid Internet Gateway (SAIG) Enrollment Agreement, which states that the institution must ensure that all federal student aid applicant information is protected from access by or disclosure to unauthorized personnel.

Because higher education institutions participate in financial activities such as making Federal Perkins Loans, FTC regulations consider them financial institutions for purposes of compliance with GLBA. Due to the efforts of NACUBO and other higher education associations, under regulations promulgated in May 2000, colleges and universities are deemed to be in compliance with the privacy provision of GLBA if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). However, colleges and universities must ensure compliance with GLBA's Safeguards Rule, which requires universities to develop a **written information security plan** that describes their program to protect customer (student) information.

At NMSU, this document, along with all of the Administrative Rules and Procedures (ARPs) included in Chapter 15 | Information Management and Data Security serve as NMSU's written information security program.

Enforcement of Cybersecurity Requirements under the GLBA

The U.S. Department of Education continues to take steps to ensure the confidentiality, security, and integrity of student and parent information related to the federal student aid programs (Cybersecurity Enforcement). Protecting that information is a shared obligation among the departments, institutions, third-party servicers, and other partners in the financial aid system. The U.S. Department of Education expects universities to maintain strong security policies and effective internal controls to prevent unauthorized access or disclosure of sensitive information.

Institutions and third-party servicers are also required to demonstrate administrative capability in accordance with 34 C.F.R. § 668.16, including the maintenance of adequate checks and balances in their systems of internal control. An institution or servicer that does not maintain adequate internal controls over the security of student information may not be considered administratively capable.

Cybersecurity Compliance

NMSU ensures compliance with data privacy regulatory requirements. Its written information security program is based on guidelines provided by the Federal Student Aid (FSA) Cybersecurity Compliance an Office of the U.S. Department of Education. It also uses technical guidelines from the Privacy Technical Assistance Center (PTAC) from the U.S. Department of Education and from the National Institute of Standards and Technology (NIST) for research-related activities.

In Dear Colleague Letter GEN-15-18 and GEN-16-12, the U.S. Department of Education reminded institutions about the longstanding requirements of GLBA and notified universities of their intention to begin enforcing legal requirements of GLBA through annual compliance audits.

Auditors evaluate/verify three information safeguard requirements of GLBA in audits of postsecondary institutions or third-party servicers under the regulations in 16 C.F.R. Part 314:

1. The institution must designate an individual to coordinate its information security program.
2. The institution must perform a risk assessment that addresses three required areas described in 16 C.F.R. 314.4(b):

a)	Employee training and management;
b)	Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
c)	Detecting, preventing and responding to attacks, intrusions, or other systems failures.

3. The institution must document a safeguard for each risk identified in Step 2 above.

At NMSU, the Chief Information Security Officer (CISO), Chief Privacy Officer (CPO)/IT Compliance Officer, and the Chief Audit Executive (CAE) are responsible for coordinating the information security program, conducting risk assessments, and appropriate document safeguards. The following sections include some general standards and guidelines to safeguard customer information.

General Standards for Safeguarding Customer Information

NMSU must meet a general standard in order to comply with the "to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards" for non-public customer information. A customer is a type of consumer, namely, an individual who has an ongoing relationship with you under which you provide a financial product or service. Therefore, our main customers are the students of NMSU.

Safeguarding objectives are:

- To ensure the security and confidentiality of customer information
- To protect against any anticipated threats to the security or integrity of such

information; and

- To guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

The required elements of the security program are:

- Designate an employee(s) to coordinate the information security program
    - The information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information
    - Identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromises of such information, and assess the sufficiency of any safeguards in place to control these risks
- At a minimum, such a risk assessment should include consideration of risks in each of the following operational areas:
    - Employee training and management
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
    - Detecting, preventing, and responding to attacks, intrusions, or other systems failures
- Oversee service providers by taking steps to select and retain providers that are capable of maintaining appropriate safeguards for customer information
- Contractually require service providers to implement and maintain such safeguards; *(NMEAF, collection agencies)* and
- Periodically evaluate and adjust the information security program based on the results of testing and monitoring

In order to comply with these requirements, the following guidelines provide the framework forthe design and implementation of an information security program.

NMSU Financial Information Privacy and Safeguarding Guidelines

Introduction

Adequately securing customer information is not only the law; it makes good business sense. Above all, it is our ethical responsibility to you, our customer as your fiduciary agent, for this information to ensure its safeguarding while in our possession. When we show you, our customer, that we care about the security of your personal information, we increase your level of confidence in our institution. Poorly managed customer data can lead to identity theft. Identity theft occurs when someone steals a consumer's personal identifying information to open new charge accounts,order merchandise, or borrow money.

Information Collected and Stored

As an educational institution, NMSU collects, retains, and uses non-public financial information about individual customers, as allowed by law, to provide services. Non-public financial information is collected from sources such as:

- Applications and/or other forms;
- Financial transactions (Checks, credit cards, and ACH)
- Information about your transactions with us, our affiliates, or others;
- Information we receive from consumer reporting agencies; and
- Information from governmental agencies.

Information Shared
NMSU may disclose non-public financial information about you with our business affiliates and other affiliated third parties under certain circumstances to provide services. Any non-public financial information sharing is conducted in strict adherence to applicable law. NMSU will not disclose any non-public personal information about you to anyone except as permitted under law.

Who Receives Information and Why
NMSU does not disclose any non-public financial information about our students/customers, or former students/customers, to anyone, except as permitted by law. However, we may exchange such information with our affiliates and certain nonaffiliated third parties (under limited circumstances) to the extent permissible under law to service accounts, report to credit bureaus, provide loan services, or provide other financial services-related activities.

How Your Information Is Protected
NMSU understands that the protection of your non-public financial information is of the utmost importance. Providing for administrative, technical, and physical safeguarding of your privacy is our obligation. We restrict employee access to customer information only to those who have a legitimate business reason to know such information, and we educate our employees about the importance of confidentiality and customer privacy. For more information on data governance and data classifications, visit Data Governance for the NMSU system | New Mexico State University.

Determining Reasonable Internal and External Threats
Determine reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

Internal Threat	Risk Level	Response
Intentional or inadvertent misuse of customer information by	Low	1) Dissemination of, and annual training, on privacy laws and university privacy policy. 2) Incorporation of privacy policy guidelines into the

current employees		employee handbook. 3) Employment agreements amended to require compliance with privacy policy and prohibit any nonconforming customer information use during or after employment. 4) Employees are encouraged to report any suspicious or unauthorized use of customer information. 5) Periodic testing to ensure these safeguards are implemented uniformly.
Intentional or inadvertent misuse of customer information by former employees subsequent to their employment	Medium	1) Require return of all customer information in the former employee's possession (i.e., policies requiring the return of all university property, including laptop computers and other devices in which records may be stored, files, records, work papers, etc. 2) Eliminate access to customer information (i.e., policies requiring the surrender of keys, ID or access codes or badges, business cards; disable remote electronic access; invalidate voicemail, e-mail, internet, passwords/passphrases, etc., and maintain a highly secured master list of all lock combinations, passwords, and keys. 3) Change passwords/passphrases for current employees periodically. 4) Amend employment agreements during employment to require compliance with privacy policy and prohibit any nonconforming customer information use during or after employment. 5) Encourage employees to report any suspicious or unauthorized use of customer information. 6) Periodic testing to ensure these safeguards are implemented uniformly
Inadvertent disclosure of customer information to the general public or guests in the office	Low	1) Prohibit employees from keeping open files on their desks when stepping away. 2) Require all files and other records containing customer records to be secured at day's end. 3) Use a software program requiring each employee to enter a unique log-in ID to access computer records and re-login when the computer is inactive for more than a predetermined amount of time. 4) Change passwords/passphrases for current employees periodically. 5) Restrict guests to one entrance point, require them to present a photo ID, sign-in, and/or wear a

		plainly visible "GUEST" badge or tag; restrict areas within the office in which guests may travel unescorted. 6) Use secure shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 7) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 8) Encourage employees to report any suspicious or unauthorized use of customer information. 9) Periodic testing to ensure these safeguards are implemented uniformly.

External Threats	**Risk Level**	**Response**
Inappropriate access to, or acquisition of, customer information by third parties	Low	1) Install firewalls for access to the university's internet site. Include privacy policy on the site. 2) Require secure authentication for internet and/or intranet and extranet users. 3) Establish dial-in protections (such as Caller-ID, Callback, encryption) to prevent unauthorized access. 4) Require encryption and authentication for all infrared, radio, or other wireless links. 5) Train employees to protect and secure laptops, handheld computers, or other devices used outside the office that contain customer information. 6) Install virus-checking software that continually monitors all files, downloads, portable media, all incoming and outgoing e-mail messages. 7) Establish uniform procedures for the installation of updated software. 8) Establish systems and procedures for secure back-up, storage, and retrieval of computerized and paper records. 9) Establish procedures to ensure external points of entry to the office are closed, locked, and inaccessible to unauthorized persons when the office is closed. 10) Install a burglar alarm or other security systems, with training for authorized persons on activation and deactivation. 11) Physically lock or otherwise secure the computer room, and if necessary, all areas in which paper records are maintained. 12) Use secure shredding machines on unused

		photocopies or other records being discarded before depositing in trash or recycling containers. 13) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 14) Encourage employees to report any suspicious or unauthorized use of customer information. 15) Periodic testing to ensure these safeguards are implemented uniformly
Inappropriate use of customer information by third parties	Medium	1) Evaluate the ability of all prospective third-party service providers to maintain appropriate information security practices. 2) Provide all third-party service providers to whom contractual access to premises or records has been granted with a copy of the Privacy Policy. 3) Require all such third-parties—by written contract—to adhere to the Privacy Policy, agree to make no use of any non-public personal information on your customers that would be prohibited thereby, or otherwise by law or contract, and agree to hold harmless and indemnify the university for any inappropriate use of customer non-public personal information. 4) Require all such third-parties—by written contract—to return all customer information and all other university property at the completion or termination, for whatever reason, of the agreement between the university and the third-party. 5) Prohibit access to customer information (i.e., policies requiring surrender of keys, ID or access codes or badges, disabling remote electronic access; invalidating voicemail, e-mail, internet, passwords/passphrases, etc., if applicable) to all such third-parties upon completion or termination, for whatever reason, of the agreement between the university and the third-party. 6) Change passwords/passphrases for current employees periodically. 7) Send "pre-emptive" notices to clients when the university has reason to believe a terminated third-party service provider may attempt to wrongfully use customer information, informing them that the agreement with the university is no longer in effect. 8) Encourage employees to report any suspicious or unauthorized use of customer information.

		9) Periodic testing to ensure these safeguards are implemented uniformly.

As a part of this commitment, we provide the following Privacy and Safeguarding guidelines:

Guideline 1 – Accountability

NMSU is responsible for maintaining and protecting the customer's financial information under its control. In fulfilling this mandate, each functional area of NMSU is required to educate its employees and comply with these guidelines. For each functional area dealing with non-public information, specific NMSU employees in each functional area must be identified as the Financial Information Privacy Custodian. This custodian is responsible for ensuring the following policies and procedures are fulfilled for their area:

Information & Communication Technologies (ICT) will perform and maintain an inventory of all information that requires protection. Custodians will contact ICT as new systems or data is being stored or if any relevant changes occur to information collection, storage, or disposal.

Guideline 2 – Purpose

The purposes for which student/customer financial information is collected shall be identified before or at the time the information is collected. If any financial information is maintained in anNMSU area, a written statement must be held in the department, stating the purpose of the information, how it is being used, the length of time it will be held, and how the information will be destroyed. Example: If the department maintains files with copies of checks or credit card information, the department must have a departmental policy on hand which states why copies are maintained, how long they are to be held, and how they will be destroyed when no longer needed.The Office of Business and Finance and ICT will work with the Custodians to help identify and state the purpose of the information collected.

Guideline 3 – Collection

The student/customer information collected must be limited to those details necessary for the purposes identified by NMSU. Information must be collected by fair and lawful means. NMSU departments may only collect the information, which is needed to perform the task at hand. Example: A department may not collect a driver's license number without a policy on hand that addresses the specific purpose and use of this information.

Guideline 4 – Use, Disclosure, and Retention

Student/customer information may only be used or disclosed for the purpose of which it was collected unless the student/customer has otherwise consented or when required or permitted by law. Student/customer information may only be retained for the period of time required to fulfill the purpose for which it was collected and will be disposed of in a secure manner when the purposehas been fulfilled. If the information is to be used for another purpose, consent must be obtained from the customer prior to use. When obtaining consent, either initially or for a revised purpose, the length of retention must be stated, and how the information will be disposed must be disclosed to the customer. Example: If a department, on a given application, maintains a driver's license number, but the department now wishes to use this information to process another application, the customer must give new consent. In the new consent, the length of time this information will be held and how the information will be destroyed must be stated. NMSU will manage private non-public information in accordance with all applicable state and federal laws relating to the use, disclosure, and retention of private non-public information.

Guideline 5 – Safeguarding

Customer information must be protected by security safeguards that are appropriate to the sensitivity level of the information obtained. Each functional area must review the information being retained and establish appropriate physical safeguards for the data. Physical paper data suchas copies of checks must be kept in locking rooms and file cabinets. Computer stored data can be protected with password/passphrase-activated screensavers by utilizing strong passwords/passphrases of at least 17 characters, by changing passwords/passphrases periodically and not posting passwords/passphrases near employees' computers, by encrypting sensitive customer information when it is transmitted electronically overnetworks, by referring calls or other requests for customer information to a designated individualwho has been trained, and recognizing any fraudulent attempt to obtain customer information and reporting it to Audit Services for evaluation. Data custodians, in conjunction with ICT will providethe training and oversight necessary to ensure the appropriate safeguarding of customer information.

Guideline 6 – Openness

NMSU is required to make information available to customers concerning the policies and practices that apply to the management of their information. Each functional area is responsible for maintaining a policy and practice document which details the financial information obtained by the department, and their adherence to these guidelines.

Guideline 7 – Access

Upon request, a student/customer shall be informed of the existence, use, and disclosure of their information and shall be given access to it. Students/customers may verify the accuracy and completeness of their information and may request that it be amended, if appropriate. Each department/unit is responsible for obtaining and presenting information when requested by a customer.

Guideline 8 – Handling Customer Complaints and Suggestions

Students/customers may direct any questions or concerns with respect to the privacy principles outlined above or about our practices by contacting the designated person(s) accountable for privacy in each NMSU department. Each department/unit is responsible for dealing with customer complaints and suggestions. Complaints and concerns may be expressed through NMSU's confidential reporting system, EthicsPoint.

Guideline 9 – Information System

Information systems include network and software design and information processing, storage, transmission, retrieval, and disposal. Security must be maintained throughout the life cycle of customer information.

- Storage of information
- Secure data transmission
- Disposal of customer information
- Erase all data when disposing of computers, or destroy hard drives containing very sensitive information
- Responding to system failure

New Mexico State University (NMSU) maintains centralized control of public and non-public data through various applications. These applications maintain their own internal security measures which are administered by the assigned data custodian for these applications. Furthermore, for 3270 access to data, a second, independent password/passphrase is required to gain initial access to the applications. This layer is known as Netview Access. A small number of Netview administrators in the Business Office and at ICT have the ability to control access to the Netview accounts. Hence, a two-tier access control is maintained for normal operation of these applications. Physical accessto the centralized computers is controlled by limited proximity card access to the data center. Weuse the centralized alarm and access security system maintained by NMSU. Access to this facilityis restricted to those who have a demonstrated need. All-access is granted by the manager of the University Computer Center.

ICT maintains secure, offsite storage of institutional data for disaster recovery purposes. This facility is located in a separate, secure location. The data tapes are kept in a locked vault inside the facility, which is set up with continuous intrusion and fire detection systems.

Data transmission of institutional data is routed through the NMSU-NET infrastructure, which is currently a switched 10/100/1000 ethernet network. For the most part, encryption of data-in-transit is made when transmitting institutional data across NMSU-NET. Physical security of the network is maintained by locked doors to communication distribution areas. Where possible, data transmission is encrypted. For example, web-based services that have non-public, authenticated data are usually encrypted using SSL.

It is our desire that all of our data be encrypted during transmission. We also have a goal that all institutional data that leaves our network be encrypted using encryption methods like P.G.P. We anticipate that in the near future, we will require such transactions to help safeguard our data from third-party intervention.

Institutional data transferred to devices is the responsibility of the end-user. All users who have access to institutional data are required to sign a document outlining their responsibility for that data. Endusers are responsible for ensuring that institutional data is securely maintained and properly destroyed.

NMSU maintains a policy for deleting all data on computers that are sold or disposed of.

NMSU maintains an IT security team to respond to problems arising from intrusions or other security violations. ICT has an assigned person to be the primary contact for such occurrences. In addition, ICT maintains a log of incidents and resolutions of all security violations.

Guideline 10 – Monitoring and Testing of Security

The information security program will need periodic evaluation and adjustment based on the result of the testing and monitoring any material changes to operation, or any other circumstances that are known to have or that may have a material impact on the information security program. AuditServices will provide assurance for the program through performance of audits on its annual audit plan.

Guiding Regulatory Technical Resources:

- The Gramm-Leach-Bliley (GLB) Act – Safeguards Rule

- Privacy Technical Assistance Center from U.S. Department of Education

- Federal Student Aid (FSA) Cybersecurity Compliance

- National Institute of Standards and Technology (NIST)

- Family Educational Rights and Privacy Act (FERPA)