Information Security Program

This document describes the program that applies to all entities and individuals, and to all systems that are used to collect, store, access, or process Personally Identifying Information (PII), whether in electronic, paper, or other forms. This program is intended to direct the actions of individuals and departments responsible for PII related to any UNM business process, but especially in demonstrating compliance with FERPA, GLBA, PCI, The Red Flags rule, and other regulatory requirements governing the security and privacy of PII.

This Information Security Program, "The Program," describes the safeguards implemented by UNM to help protect PII. All information and information systems that are part of the collection of processing of PII must comply with this program and administrators of those systems are responsible to develop the supporting controls and documentation indicating compliance with this program.

These safeguards are provided to:

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

This Information Security Program also identifies mechanisms to:

• Identify and assess the risks that may threaten PII collected and maintained by UNM;
• Develop written policies and procedures to manage and control these risks;
• Implement and periodically review the program; and adjust the program to reflect changes in technology, or UNM practices regarding the collection, storage, access, or processing of sensitive information, and with respect to internal or external threats to information security.

UNM has appointed Information Security Program Coordinators to conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to PII, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Information Security Program Coordinators

The University Controller, The University Provost, and the University CIO are the coordinators of the program. They are responsible for assessing the risks associated with unauthorized access to PII, and for implementing controls to minimize those risks. The University Compliance Officer Internal will review and assess the Policies, Procedures, and other administrative controls for entities that handle PII. Internal Audit personnel will conduct periodic reviews of areas that access PII.
Identification and Assessment of Risks to Customer Information

UNM recognizes that it is exposed to both internal and external risks, including but not limited to Unauthorized Access to PII:

- Due to a compromised computing system
- Interception of PII during transmission
- Loss of data integrity in a technical safeguard or control
- Physical loss from theft
- Unintentional errors introduced into the system
- Corruption of data or systems
- Through unauthorized requests
- Through hardcopy files or reports
- Through unauthorized third parties

Recognizing that this may not represent a complete list of the risks associated with the protection of PII, and that new risks are created regularly, the UNM Compliance Officer and the CIO of UNM will actively participate and monitor appropriate advisory groups and regulatory bodies to keep apprised of evolving risks.

To help ensure that the current safeguards implemented, monitored, and maintained by UNM are reasonable, the CIO of UNM will periodically schedule third party assessments of the those controls, and will make periodic adjustments to those controls to respond to changes in the threat landscape.

Notification

Any breach, suspected breach, or security event or incident that could indicate a breach of PII must be reported immediately upon discovery to UNM Information Security at security@unm.edu or to the Customer Support Services (CSS) at 277-5757. These reports will also be delivered to the University Compliance Officer. Summary reports of incidents and breaches will be provided to the CIO, the UNM President, and to the Executive Vice Presidents on a quarterly basis.

Compliance Reporting

Information Security Program Coordinators and appropriate business units will submit their standard operating procedures (SOPs), risk assessments and operational control information, as well event and/or breach notification, to the University Compliance Officer. Any departmental or business policies must be published.

Employee Management and Training

Background checks of new employees working in areas who may access PII in their regular job duties, such as the Bursar's Office, Financial Aid, and Information Security, will be performed. During new employee orientation, each employee in departments that access PII in their regular job duties will receive training on the importance of confidentiality of student records, financial information, and other PII.

Each new employee in areas who will access PII in their regular job duties will also be trained in basic information security practices related to the department's business practices. For such employees, this training will include a review of the departmental controls and procedures that prevent employees from providing PII to an unauthorized individual, as well as training on how to properly dispose of records that contain PII. These training efforts are intended to help minimize risk and safeguard PII.
Physical Security

UNM has addressed the physical security of PII by limiting physical access to PII to only those employees who have a legitimate business need to access such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are made available only to UNM employees with an appropriate business need for such information.

Furthermore, each department responsible for maintaining PII is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or due to technical failures. Employees who access or manage information systems will also be trained on their departmental procedures governing physical access to servers, workstations, networks, network devices and cabling, etc., as well as the appropriate audit trails for such systems.

Information Systems

Access to PII via UNM information system is limited to those employees who have a legitimate business need to access such information. Departments with systems that store, access, or process PII must have policies and procedures in place to complement the physical and technical safeguards in order to provide security to UNM information systems. Those policies, procedures, and safeguards must be provided to the UNM Compliance Officer.

Among other information, Social security numbers (SSNs) are considered PII. As such, UNM has discontinued the use of SSNs as student identifiers in favor of the Banner ID as a matter of policy. By necessity, SSNs will remain in UNM information system; however, access to SSNs is granted only in cases where there is an approved, documented business need. Access to SSN should only be provided in accordance with federal regulatory reporting requirements, such as Student Financial Aid, Federal Income Tax Reporting, etc.

Management of Information Security Failures

The Information Security Office has developed incident response plans and procedures to help detect and prevent breaches of PII on UNM enterprise information systems. Departments that store, access, or process PII must also have incident response plans and procedures in place, and these must be submitted to the UNM Compliance Officer. Internal Audit personnel will conduct regular reviews of such plans and procedures in order to assure that they are adequate for the protection of the PII on those systems, or for paper or other non-electronic records.

Oversight of Service Providers

UNM will take reasonable steps to select and retain service providers who maintain appropriate safeguards for PII. This Information Security Program will help ensure that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. Individuals and departments will identify service providers who have or will have access to PII, and will work with the Office of University Counsel, with UNM Purchasing, and with other offices as appropriate, to help ensure that service provider contracts contain appropriate terms to protect the security and privacy of PII. Internal Audit personnel will conduct reviews of such service providers and contracts in order to assure that the control structures put in place for service providers are adequate to protect any PII made available.

Continuing Evaluation and Adjustment

This Information Security Program will be subject to periodic review and adjustment. Continued
administration of the development, implementation and maintenance of the program will be the responsibility of the Information Security Program Coordinators, who will assign specific responsibility for technical, logical, physical, and administrative safeguards implementations and administration as appropriate. The Information Security Program Coordinators, in consultation with the Office of University Counsel, will review the standards set forth in this program and recommend updates and revisions as necessary; it may be necessary to adjust the program to reflect changes in technology, in what constitutes PII, and/or internal or external threats to information security.

**Covered data and information**

For the purpose of this program, covered data specifically includes student financial information (defined below), UNM LoboCash information and any and all sensitive data, including credit card information and checking/banking account information received in the course of business by UNM. Covered data and information includes both paper and electronic records.

**Student financial information**

Student financial information is that information that UNM has obtained from a student or customer in the process of offering a financial product or service, or such information provided to UNM 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. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and SSNs, in both paper and electronic format.

**Related Policies, Standards and Guidelines**

UNM has adopted comprehensive policies, standards, and guidelines relating to information security, which are incorporated by reference into this Information Security Program. They include:

**Policies**

- UNM SSN Policy: policy.unm.edu/university-policies/2000/2030.html
- UNM Credit Card Processing Policy: policy.unm.edu/university-policies/7000/7215.html

**Departmental Policies**

Departmental Policies are allowed provided they refer to this policy, that they are at least as restrictive as this policy, and that any reporting requirements are enforced.

**Standards**

- Information Classification Standard: cio.unm.edu/standards/
- Information Stewardship and Confidentiality Document: cio.unm.edu/standards/
- Data Encryption Standard: cio.unm.edu/standards/