

UNM Sensitive Information Stewardship Statement

1. It is the practice of the University of New Mexico (UNM) to promote **data stewardship**, ensuring the **confidentiality, integrity, and availability of sensitive information**. You are asked to sign this statement because your job duties may require that you have access to sensitive information. The purpose of this statement is to reaffirm your responsibility to help protect sensitive information. UNM reserves the right to take disciplinary action, up to and including termination, for violation of the confidentiality obligations identified in this statement. Your permission to access sensitive information and information systems, or any other institutional systems interfaced to such systems, is subject to your agreement to adhere to the following terms and conditions:
2. I understand that helping to maintain the confidentiality, integrity, and availability of sensitive information is a requirement of my job. Any unauthorized disclosure or alteration of sensitive information that is a result of my negligence or oversight would cause substantial damage to the rights of those individuals whose data is stored, and would also cause damage to UNM.
3. I understand that sensitive information may be legally confidential by virtue of the Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 1232g), by the Health Insurance Portability and Accountability Act (HIPAA), and / or by other privacy laws. Under these privacy laws, I may not disclose sensitive information about UNM employees, about students, or about patients unless I am advised by policy or by written guideline that such disclosure is permitted in particular circumstances.
4. I will use UNM information systems and the sensitive information they contain solely for the purpose of conducting UNM business. Access to, or use of UNM information systems, or the sensitive information those systems contain, for my own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity, is strictly forbidden. I also understand that it is impermissible to revise any records even if the records relate to me, or to a family member, or to a friend, except at the direction of the appropriate administrator for such records, and only to serve the business purposes of UNM.
5. I will only share sensitive information with persons to whom authorization is granted and only for UNM business purposes. I understand that the University expressly forbids the disclosure or distribution of sensitive information in any medium, except as required by my job duties and responsibilities, and only to serve the business purposes of UNM.
6. I will prevent the disclosure of my access codes and / or passwords to other individuals. I will not use others' access codes and / or passwords, even with their permission. If I have reason to believe that my access codes and / or passwords, or those of another individual have been compromised, or are being used by a person other than the individual to whom they were issued, or are being used for any illicit purpose, I will report it to a supervisor, or to the UNM IT Security administrator security@unm.edu, or anonymously using the Information Security Hotline at 505-277-0930. Those accounts used for maintaining departmental web pages, for shared calendars, etc., are allowed exceptions to the non-disclosure requirement of this rule.
7. I will help prevent unauthorized access by abiding by all account and password management standards established for my organization. These standards may include requirements for password complexity, requirements for the frequency of password changes, and / or requirements of a formal approval process for the creation of new accounts on UNM information systems.
8. I understand that I will be held accountable for the consequences of any misuse occurring through computer accounts for which I am responsible, and due to any neglect or negligence on my part. For example, if I leave my workstation for any reason, I will initiate appropriate security measures (e.g., a password protected screensaver) so that no unauthorized person may access or enter information under the authorization of my security codes and / or passwords. I will make sure the system screen and any paper records with sensitive information are not left open or unattended in areas where unauthorized individuals may view them.
9. My signature on this document signifies that I have carefully read and understood the terms and conditions of this Information Confidentiality Statement, and acknowledge that my continued employment at or through UNM is dependent upon my strict adherence to all of its terms and requirements.

Print Employee Name: _____

Signature:

Print Supervisor Name: _____

Signature:

Glossary

Data Stewardship refers to industry best practices in the treatment of information in the context of its sensitivity as an institutional asset.

Confidentiality refers to the treatment of sensitive information that must never be disclosed to those individuals without a UNM Business-related need to access or modify such information. I may not disclose confidential information about UNM employees, about students, or about patients unless I am advised by policy or by written guideline that such disclosure is permitted in particular circumstances.

Availability refers to the ability of those with a UNM business-related need for access to or modification of sensitive information to have that access when it is required.

Integrity refers to the viability of sensitive information, such that it is not subject to repudiation, based on its accuracy or currency.

Information Systems refers to computer workstations and servers, applications, databases, and the information that resides upon or in them.

Sensitive information, whether in electronic or physical forms, includes, but is not limited to the following:

1. **Personal and financial records**, including home address, home phone number, SSN, banking, loan, and credit and / or credit card information, and employment applicant information;
2. **Patient health information**, including records of patient illnesses and treatments, and insurance and related financial information;
3. **Student records**, including grades, courses taken, fields of study, and programs in which the student is enrolled, and exams and quizzes, and other related academic record information;
4. **Privacy Flagged records**, including *any* information about an individual who has set a privacy flag on a University information system.

Sensitive information also includes:

1. Records subject to **export control regulations**;
2. Records related to **UNM legal actions**;
3. Records related to **law enforcement actions**;
4. Records related to **UNM HR actions and / of personnel records**;
5. Records related to **the security of UNM records and / or information systems**.

Sensitive information:

Should never be stored locally, but **must** be encrypted if it is temporarily stored locally.

Should always be stored in approved secure locations.

Should never be stored on removable media.

Should never be removed from the workplace.