65-7 Confidentiality of Records

65-7-1 Purpose • 65-7-2 Policy • 65-7-3 Definition • 65-7-4 Administration • 65-7-5 Applicable Law • 65-7-6 Responsibilities of Users • 65-7-7 Examples of Violations • 65-7-8 Sanctions

1. **Purpose.** The purpose of this policy and procedures is to assure that confidential or personal identification information about students or employees of Eastern New Mexico University System (the System) is secured, access is limited and appropriate, and that information does not leave campus in paper or electronic form.

2. **Policy.** The ENMU System general policy is as follows:

   A. The System has the right to limit access to educational records to System officials with a legitimate educational interest, such as an employee performing a task that is specified in her/his position description, providing a service of financial aid, maintaining the safety or security of the System, compiling data for federal, state, or other accreditation reporting, or collecting data for institutional research.

   B. Unauthorized disclosures or acquisitions of private data, known and suspected, must be reported to the System officials immediately.

   C. The System has the right to share information to others with legitimate educational interest; persons operating under a judicial order or lawfully issued subpoena or law enforcement; or, in an emergency, with others when information is necessary to protect the health or safety of the students or other persons.

   D. The System has the right to require that educational records and System records remain secured at all times.

3. **Definition**. For purposes of this policy, confidential or personal identification information about students or employees includes any records in which names or numbers, alone or in conjunction with any other information, can be used to identify specific individuals.

The foregoing purposes and policies shall be implemented using the following.

Guidelines and Procedures

4. **Administration.** These policies, procedures and guidelines shall be administered by the vice president for Student Affairs and the ENMU System chief financial officer (CFO).

5. **Applicable Law**. In compliance with Section 438 of the "General Education Provisions Act" (as amended) entitled "Family Educational Rights and Privacy Act of 1974" (FERPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the System recognizes its obligation to provide appropriate access to educational records while protecting their confidentiality.

6. **Responsibilities of Users**. Due to the integrated nature of various information access modules, employees may have access to a wide range of data while performing their contractual obligations. Therefore, users shall abide by the following guidelines:

   A. Users shall not disclose or store passwords or data in an unsecured manner.

B. Users shall not share confidential and sensitive information with anyone, including colleagues, without a legitimate educational reason.

C. Users shall not leave a desk or computer station unattended while logged on to administrative information systems.

D. Users shall maintain, secure and shred (as needed) printed reports that contain confidential or sensitive information.

E. Users shall not remove confidential materials, reports, or documents, printed or electronic versions, from the work area. Users may not store confidential information on laptops or other electronic storage devices that will leave the designated work area.

7. Example of Violations. Following are examples of violations for which System disciplinary action may be taken. This list is not intended to be comprehensive.

A. Misuse of computer access passwords (sharing or posting passwords, unauthorized use of others' accounts, allowing use of accounts by others, etc.)

B. Attempting to bypass or exploit physical or technical security measures.

C. Accessing confidential data outside the scope of one's professional "need to know," for personal curiosity, financial gain, or as a favor for someone else or the unauthorized publishing of private data in any medium.

D. Storing confidential data or information on laptop computers or removable computer media (disks, CD's, tapes, keys, portable memory storage devices, etc), unless the storage is required for work and remains secured at the work site.

E. Selling private data.

F. Unauthorized disclosure of private data to persons without a "need to know" either deliberately or accidentally (i.e. leaving documents containing private data unattended in public places, posting private data on unsecured web sites, sending data in emails outside the system, misplacing or otherwise losing personal identification information).

8. Sanctions. Given the serious nature of the misuse, unauthorized removal or loss of confidential records or System information, an employee responsible for any infraction of this policy may be subject to disciplinary action, whether the action is accidental or intentional.

Approved by Board of Regents on September 13, 2007
Revisions approved by the Board of Regents, November 1, 2019