Reporting Policy

1.0 Overview

University employees with a legitimate educational interest may routinely have access to confidential student data as provided by the Family Educational Rights and Privacy Act (FERPA). This includes faculty, staff, administrators, and student employees working in the division of UNO Enrollment Services and other limited campus offices directly involved in student advising and enrollment services.

Effective security is a team effort involving the participation and support of every university employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to protect the confidentiality and integrity of student records by educating users of their responsibilities and proper usage guidelines.

3.0 Scope

The scope of this policy includes all university employees authorized to view and run reports.

4.0 Policy

4.1. Authorization

Any employee requesting access to reporting software must request the access in the Peoplesoft Account Request system (http://psaccount.unomaha.edu). The request must be signed by three accountable individuals: the direct supervisor of the individual making the request; the UNO Data Steward for the University; and the UNO Security Administrator. Access to reporting software will be created by Information Services employees after proper approval from all three individuals.

4.2. Usage

Reporting access may be used for legitimate University related functions only. All user accounts are subject to relevant UNO and UN System policies and the following provisions:

4.2.1. Information cannot be harvested from ad hoc reporting software

4.2.2. Information cannot be used in any other third party system.

4.2.3. Information provided is for official University business only. It is not to be shared outside of the University without approval.

4.2.4. Financial data provided to the university by students and their families is not available for reporting purposes.

4.3. Re-disclosure

The Family Educational Rights and Privacy Act mandates that student academic records are to be kept in confidence. Re-disclosure of records are bound to the following provisions:

4.3.1. Material containing personally identifiable information may **NOT** be re-disclosed to another party without the student's written consent.

4.3.2. *Non-directory information* cannot be disclosed to a third party without the student's written consent.

4.3.3. Unless written permission is obtained, the discussion, use or access of student records is limited to job-related legitimate educational interests. This includes reports, e-mails, and extracts containing student record information.

4.3.4. Extracts must be approved by the UNO Data Steward and coordinated with the UNO SIS Security Administrator

4.4. Disposal

Material containing personally identifiable information must be handled in a confidential manner. The information should not be left in an open area or left unattended at any time. Once the initial purpose

for which the information was produced has been met, the material containing personally identifiable information must be properly disposed of.

4.4.1. Electronic copies of data must be securely deleted using *secure delete*

4.4.2. Web-browser software should be exited to clear the cache

4.4.3. Lists and labels should be shredded or disposed of in a similar, secure manner

4.4.4. Email containing student information must be deleted after intended use is met

4.5. Related University Policies

4.5.1. Family Education Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

4.5.1.1. All users must adhere to FERPA. All users are expected to know this law. More information can be found at http://www.ses.unomaha.edu/registrar/ferpa.php

4.5.2. Regent Bylaws

Board of Regents Bylaw section 5.6 defines "directory" and "non-directory" information for the University as it pertains to student records, in compliance with FERPA. The policy can be reference on the NU website at: http://nebraska.edu/docs/board/bylaws.pdf

4.5.3. Memorandum 16

It is the purpose of this Executive Memorandum to set forth the University's administrative policy and provide guidance relating to responsible use of the University's electronic information systems.

4.5.4. Restricted Data Policy

University data that is highly confidential and is covered by State or Federal privacy law. The policy can be referenced on the UNO website at: http://www.unomaha.edu/policies/docs/Restricted%20Data%20Security%20Policy%20v1.0-final.pdf

5.0 Enforcement

Any violations of this policy may include, but is not limited to, termination of access to reporting software.

6.0 Definitions

6.1. Secure Delete is the process of overwriting information on a computer hard disk with random information so that it cannot be recovered by software.

6.2.

7.0 Revision History

Date	Section	Change	Who
7/14/2010	Document Created	None	Andrew Throener