Student Information System Security 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 with a legitimate business need to access the University of Nebraska at Omaha's Student Information System.

4.0 Policy

4.1. Access Policy

Before access is granted to the student information system, the request must be approved by three accountable individuals, the head of the department making the request, the *data steward*, and the *SIS security administrator*.

4.1.1. Access is provided to the Student Information System based on a security best practice known as **least privilege security principle**. Users are granted access only to the information deemed necessary to perform their job duties.

4.1.2. Additional access may be provided if deemed necessary to perform job duties.

4.1.3. SIS account credentials are created for one user only.

4.1.4. Credentials are considered confidential, sensitive information and are not to be shared to anyone.

4.1.5. Credentials are not to be written down.

4.1.6. Credentials are not to be embedded in any script or program. This includes web browsers and password storage programs.

4.1.7. Accounts inactive for 20 months will be disabled.

4.1.8. Users must sign out of the student information system when not in use.

4.1.9. Users must not leave an open connection to the student information system unattended.

4.2. Redisclosure Policy

The Family Educational Rights and Privacy Act mandates that student academic records are to be kept in confidence.

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

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

4.2.3. 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.

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

4.3. Disposal Policy

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.

4.3.1. Electronic copies of data must be securely deleted using *secure delet*e (*bit writing) software*.

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

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

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

4.4. 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.

4.4.1. All student information systems 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. Regent Bylaws

4.5.1. 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

4.6. Ad Hoc Reporting

Employees with a current SIS account may request access to the universities ad hoc reporting software. All policies associated with an SIS account apply to ad hoc reporting software in addition to the following considerations:

4.6.1. Information cannot be harvested from ad hoc reporting software.

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

5.0 Procedures

5.1. SIS Access request

Before access is granted to the student information system, the request must be approved by three accountable individuals, the head of the department making the request, the *data steward*, and the *SIS security administrator*. The access request application can be found at http://psaccount.unomaha.edu. To gain access to the student information system the following procedure must be followed:

1. To be eligible for a SIS account the employee must have gone through the full hiring process and been issued a valid university email account and network identification.
2. The head of department must login, using UNO NetID and password, and submit an access request.
3. The request must then be approved by the *data steward.*
    a. The data steward reserves the right to change the request or deny the request.
4. The request must then be approved by the *SIS security administrator*.

a. The security administrator will sign the request and define which policies need to be signed by the user.
b. The security administrator reserves the right to change the request or deny the request.

5. The user then logs in verifies the accuracy of the request and signs the appropriate policies.
6. The *SIS security administrator* creates the account.

5.2. SIS Access Revocation

If an employee's actions are deemed inappropriate in any way a formal report is filed with the *UNO SIS Security Administrator*. The *UNO SIS Security Administrator* works with the *UNO SIS Data Steward* and other security personnel, as needed, to assess the appropriate action.

5.3. SIS Access Recertification

Account access inactive for a period of 20 months will be automatically disabled. Employees must go through the access request procedure defined in section 5.1 in order to regain access to the student information system. All SIS account access must go through an annual recertification in order to assure employee comprehension and compliance with current UNO Student Information System policy.

6.0 Responsibilities

6.1. Employee Responsibility

It is the responsibility of the employee to understand and comply with this policy

6.2. UNO SIS Data Steward Responsibility

It is the responsibility of the data steward to understand and comply with the laws and regulations that apply to the data.

6.3. UNO SIS Security Administration Responsibility

It is the responsibility of the security administrator to work with the data steward and other information security personnel to protect the confidentiality and integrity of the data.

7.0 Guidelines

It is imperative that each employee or recipient understand and accept the responsibility of working with confidential student records. The access to UNO Student Records can be very limited for some employees and very broad for others, depending on their business need. In any case, one should always limit the exposure to confidential student records. The following are some examples of inappropriate use of student records:

1. Posting grades publically using the student ID (SSN). Please use an identifier that the student chooses privately, so as to not be in a personally-identifiable form.
2. Discussing student records with any person without a legitimate education need-to-know. This pertains to discussions on and off the job, and in e-mail communications.
3. Removing any document from the office for non-business purposes. Confidential student academic records should not be taken home in any and all forms (including, but not limited to, printed documents, saved electronic reports, USB flash drives and other portable media).
4. Accessing or reviewing a student's academic record without legitimate education interest (need-to-know).
5. Releasing any *non-directory* student information to any individual (including parents) without the student's written permission.
6. Releasing any *non-directory* student information to any student or University organization without the student's written permission.
7. Leaving reports or computer screens containing confidential student information in view of others who do not have a legitimate education interest in the data.
8. Making personal use of student information.
9. Allowing another person to use your computer access code.
10. Leaving your computer terminal unattended if "logged on" to a student database past the point of sign on and security procedures.
11. Embedding your computer access code in a web browser or automatic sign-on script.

8.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including access revocation and termination of student information access.

9.0 Definitions

9.1. Directory Information

Directory information is defined in the Board of Regents Bylaws, section 5.6. It includes the student's name, dates of attendance, degrees granted, date of degrees, college, major, class standing, campus and permanent addresses and phone numbers, participation in officially recognized activities and sports, and most recent educational agency or institution attended.

9.2. Non-Directory Information

Information not deemed as directory information.

9.3. Bit Writing Software

Software that securely deletes data by randomly writing bits to disk storage where the deleted information resides. Examples include Eraser and Data Shredder.

9.4. Credentials

The username and password combination used to access the student information system.

10.0 Revision History

Date	Section	Change	Who
5/22/2008	**All**	**Document Created**	**athroener**