

SOUTHWESTERN UNIVERSITY ELLUCIAN SECURITY AND ACCESS POLICY

Purpose

The purpose of this policy is to establish measures for security, access, and use of the Southwestern University administrative system known as Ellucian. This system is a shared integrated database and therefore it is important to emphasize that this policy ensures availability of information across divisions. The system is not to be used for any other reason than the access and management of administrative information

Those Affected By This Policy

All Southwestern University faculty, staff, and students are directly affected by this policy.

References

Data elements in the Ellucian system and their confidentiality, use and release are also governed by established university policies and federal and state laws, including the following (see appendix):

- FERPA of 1974 as amended (Also known as Buckley Amendment)
- Staff Handbook – Professional Expectations, Confidentiality

This policy is intended to address only security and access and does not supersede in any way other established policies and regulations.

Policy

The Ellucian system at Southwestern University consists of six modules: Finance, Human Resources, Student, Core, Utility, and Alumni/Development. Each of the modules has a designated functional access liaison who is responsible for approving access. As a general principle of access, University data shall be shared only among Ellucian users whose work can be done more effectively by knowledge of such information.

The functional access liaison is accountable in collaboration with the security administrator for ensuring that each Ellucian user knows the responsibilities placed on them by this policy. User IDs are assigned by the security administrator in ITS Administrative Computing to authorized users after completion of Ellucian UI navigation training.

Ellucian users are not to share their user IDs with anyone. If it is found that user IDs are being shared, users are subject to disciplinary action in accordance with current University regulations dealing with the activities and behavior of students, faculty, and staff.

An approved *Ellucian Access Application*, which indicates agreement with adherence to security and access policies of the University, is required of each Ellucian user. The functional access liaison and user's department head are to ensure that the level of access is consistent with the user's job responsibilities. Access should be narrowly defined so that it is just sufficient for the user to effectively perform their duties.

In general, all Ellucian information must be treated as confidential. Even public or "directory" information is subject to restriction on an individual basis. Unless your job specifically involves

release of information and you have been trained in that function, any requests for disclosure of information, especially from outside the University should be referred to the appropriate office.

Procedures

1. To request access, a new user acquires a *Ellucian Access Application* from ITS Administrative Computing or supervisor. The form must be completed and signed by the user with assistance from the department supervisor to determine the appropriate access for the user. The form is then approved by the supervisor and functional access liaison, if applicable, and sent to the security administrator.

A copy of the Southwestern University *Ellucian Security and Access Policy* is to be given to each user.

Note: The security administrator in ITS Administrative Computing maintains a list of people who are the functional access liaisons. If the functional access liaison is to be absent for a period of time the alternate's name and the period of time is to be communicated to the security administrator.

2. To change access for existing users, the approved form is sent to the security administrator in ITS Administrative Computing who updates the access in accordance with the form.

3. The security administrator will maintain a historical file of all authorized forms.

4. The department head is to notify the security administrator of users who have terminated employment or changed positions. As a crosscheck, Human Resources provide a list of terminations and changes of employee responsibility biweekly to the security administrator. The security administrator will verify that user's account has been changed or deleted.

5. Student access accounts are to be deactivated when the student withdraws or graduates, changes labor positions, or at end of spring term, unless the student is working during the summer at the same labor position. To disable the account, the supervisor submits a *Ellucian Access Application* to the security administrator.

When a student returns, the supervisor completes a *Ellucian Access Application* indicating the account to be reactivated. If the student does not return to the position, the supervisor completes a *Ellucian Access Application* terminating the account. The form is to be signed by the student, approved by the department head, and sent to the security administrator. Upon receiving the form, the security administrator reactivates the account and notifies the department head.

Note: Department heads are to maintain a list of student access accounts and names of students that are currently assigned to each account.

Functional Liaisons				
Module	Liaison	Extension	Location	Alternate Liaison
Admissions	Christine Bowman	1202	Adm	Scott Sandoval
Development	Paul Secord	1235	CB 30	Kent Huntsman
Financials	Brenda Thompson	1442	CB 112	Lenora Chapman
Financial Aid	James Gaeta	1202	Adm	Christine Bowman
Human Resources	Elma Benavides	1441	CB 142	Brenda Thompson
Student	Sean Smith	1186	PRC 108	Julie Cowley

APPENDIX

U.S. Department of Education

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) 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.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
 - School officials with legitimate educational interest;
 - Other schools to which a student is transferring;
 - Specified officials for audit or evaluation purposes;
 - Appropriate parties in connection with financial aid to a student;
 - Organizations conducting certain studies for or on behalf of the school;
 - Accrediting organizations;
 - To comply with a judicial order or lawfully issued subpoena;
 - Appropriate officials in cases of health and safety emergencies; and
 - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual

means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information or technical assistance, you may call (202) 260-3887 (voice). Individuals who use TDD may call the Federal Information Relay Service at 1-800-877-8339.

Or you may contact us at the following address:

Family Policy Compliance Office

U.S. Department of Education

400 Maryland Avenue, SW

Washington, D.C. 20202-5920

Staff Handbook (August, 2009)

II. PROFESSIONAL EXPECTATIONS

D. CONFIDENTIALITY

All Southwestern University's records and information relating to Southwestern University or its constituents are confidential and employees must, therefore, treat all matters accordingly. No information related to Southwestern University, including but not limited to, documents, files, records, computer files or similar materials (except in the ordinary course of performing duties on behalf of Southwestern University), may be removed from the University's premises without permission from Southwestern University. Additionally, the contents of the University's records or information otherwise obtained in regard to business may not be disclosed to anyone, except where related to the University's business. Employees will be subject to appropriate disciplinary action, up to and including termination/dismissal, for revealing information of a confidential nature. Please note that employee pay rates, salaries and/or any form of employee compensation are considered to be confidential and any employee divulging such information will be subject to this same disciplinary action.

In the course of an employee's work, he/she may have access to confidential information regarding the University, students, and/or fellow employees. It is imperative that no individual, in any way, reveals or divulges any such information and that it is used only in the performance of their duties. Any questions from a visitor or telephone caller about University policies or individual students or faculty should be referred to the University Relations department. Questions relating to personnel matters and matters involving potential litigation against the University, its employees or its students should be referred to the Associate Vice President for Human Resources.

Student Record information is especially sensitive, and is also protected by the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended. Employees handling any inquiries about students or working with information about students must be familiar with relevant sections of the Southwestern University Catalog, Student Handbook, Faculty Handbook, and Advisor Handbook. Employees should never release student information without being sure of the rules.