Auburn Montgomery

Title: Computer Access to Student Records

Responsible Office: Information Technology Services

I. Purpose

To establish the general structure for which data are made accessible to data users in compliance with FERPA (Family Educational Rights and Privacy Act of 1974).

II. Policy

Auburn Montgomery has determined that information in student record files can be changed only by authorized personnel in the following areas: Enrollment Services Office authority to change demographic and academic history data; Financial Aid Office authority to change financial aid data; Student Service Center authority to change student account data. All other personnel, with the exception of those with administrative authority for the management of information, have "registration" and/or "inquiry" access only.

III. Effective Date

January 5, 2007

Revised Date

May 15, 2007

IV. Applicability

Personnel in the following areas:
Demographic and Academic History: Enrollment Services Office
Financial aid: Financial Aid Office
Student accounts: Student Service Center
All other personnel with the exception of those with administrative authority for the management of information have "registration" and/or "inquiry" access only.

V. Responsibility

The Chief Information Officer in Information Technology Services in coordination with the designated contacts in Enrollment Services, Financial

Aid, and the Student Service Center implements and administers the policy/procedure in detail.

VI. Definitions

Inquiry access is a tool by which certain information stored on computer files may be viewed on a computer terminal/PC. Inquiry access allows authorized user the opportunity to view information on specific students and courses. Information cannot be updated with Inquiry access.

VII. Procedures

1. Written requests for computer access to information must be initiated by the immediate supervisor of the employee desiring access and must be submitted to the Chief Information Officer (CIO). An employee desiring access to Student Banner®, must complete an AUM- User Access Request Form. The completed form should be returned to the Office of Enrollment Services. Approval for access will be evaluated based upon a legitimate need to know.
2. Immediate supervisors will serve as a point of contact with the CIO for matters concerning data access and security. Supervisors will be asked to participate in meetings scheduled to discuss new developments and/or update information.
3. Before approving computer access to data, the CIO requires that the form "Request for Account on Administrative Computer" be completed for each individual who is to have access.
4. The immediate supervisor sends the completed form to the Office of Information Technology Services, attention: CIO. It is expected that only the person identified on the request form will have access to the system; therefore, access must be requested for each person in order to maintain system security. Access is issued to people, not positions or workstations.
5. Prior to the approval of access, the CIO will arrange an orientation session for individuals who have been approved for access. This orientation will include both general information and information concerning the confidentiality of data.
6. The form "Acceptance of Responsibility" must be signed upon the completion of the orientation session and attached to the request for access.
7. Persons approved for access are responsible for the security of their passwords and the protection of information. The authority to access is linked to a person's user ID. At no time should individuals share their passwords with another person, display the password in public view, or install the password as a macro function. Persons approved for access are responsible for signing off when finished with access.

8. Persons with access will use information ONLY for the purposes approved and will not release information to any other individual or office for another purpose.
9. All persons access confidential or restricted student data must guarantee to maintain data about individual students in a secure manner, such that it cannot be viewed by screen access, by file access, or in printed form, by unauthorized individuals. Although it is allowable to print a report or screen of confidential information for authorized record keeping or advising purposes, users should not release printed information to other individuals or offices. Any personally identifiable confidential data contained in print form or on computer files which are no longer needed should be destroyed in such a way that identification of a student is not possible.
10. All persons with access must read and sign an agreement acknowledging an understanding of their responsibilities for password security and maintaining the confidentiality of data that is accessed. This signed agreement is kept on file in the office of Information Technology Services.
11. Persons with access are also responsible for terminal/PC equipment security, which includes password sign-on and sign-off procedures and the proper placement of the equipment so that the screen cannot be viewed from a public location.
12. Supervisors of departments or units are responsible for maintaining the overall security of access and the release of information in their areas. As personnel changes occur supervisors must notify the CIO of Information Technology Services, CIO in order to initiate access deletion when a staff member terminates employment or transfer to another department.
13. If a security violation is detected, employees must contact their supervisors immediately. Supervisors are responsible for contacting the CIO of Information Technology Services, to request that passwords be changed.
14. Computer access to information in student record files will be reviewed annually by the CIO of Information Technology Services, Senior Director of Enrollment Services/Registrar, and Dean of Students.
15. Questions regarding assistance with computer equipment and passwords should be directed to the CIO of Information Technology Services. Questions about specific access to information or interpretations of FERPA should be directed to the Registrar.

VIII. Sanctions

1. Persons have access to student records should be aware that there are possible civil sanctions and university disciplinary action for violating records privacy agreements.

IX. Exclusions

Personnel in the following areas:
Demographic and Academic History: Enrollment Services Office
Financial aid: Financial Aid Office
Student accounts: Student Service Center
All other personnel with the exception of those with administrative authority for the management of information have "registration" and/or "inquiry" access only.

X. Interpretation

The CIO of Information Technology Services will interpret the policy if needed.

Approval to Proceed: _____ Date:_____

Auburn Montgomery
Information Technology Services

Acceptance of Responsibility
Computer Access to Records

I understand that my acceptance of access to information in student record files signifies that I assume responsibility for complying with the policy of Auburn Montgomery that protects the privacy of that information and the release of that information. I have received copies of and have read the policies "Computer Access to Records: and the Student records Policies and Procedures." By my signature below, I understand and agree to preserve the security and confidentiality of information I access.

I also agree to inform my immediate supervisor, who will inform the CIO of Information Technology Services, when my need to access information in student record files ceases to exist or changes in any way.

I understand that I am responsible for the personal security of my password and that there are possible civil sanction and university disciplinary actions for violating records privacy agreements.

_____ _____
Signature of Employee Date

As supervisor for this employee, I assume responsibility for the following: arranging attendance at orientation sessions, informing the CIO of Information Technology Services, of any changes in the status of this employee, and initiating access deletion if this employee leaves the current position for which he/she given access approval.

_____ _____
Signature of Supervisor Date

Auburn Montgomery
Information Technology Services

REQUEST FOR ACCOUNT ON BANNER ADMINISTRATIVE SYSTEM

I,_____, hereby request an account on the administrative computer system at Auburn Montgomery. I understand that the student records maintained on this system are confidential and are protected by the Federal Family Educational Right and Privacy Act, known as FERPA, and the Buckley Amendment. I may be liable to legal action for any breach of this document. I agree to use my account on this computer system for legitimate, authorized purposes and to exercise caution when accessing confidential information contained therein. I will ensure that no unauthorized person gains access to this information using my account. I agree to safeguard the password for my account and to log off the system when I am not using it. I will not permit any other individuals use of my account, whether or not I actually entered it. Finally, I agree to report immediately any breach of security involving my account to Auburn Montgomery Information Technology Services.

_____ _____
Requestor's Signature Date

_____
School and or Department

_____
Job Responsibility or Title

_____ _____
Signature of Supervisor Date

AUM-BANNER USER ACCESS REQUEST

Please note: This form cannot be processed unless all (*) asterisked fields are filled.

USER INFORMATION

*USER NAME (Last, First, Middle) _____

*IMMEDIATE SUPERVISOR _____

*JOB TITLE – Indicate if this is a new job title _____

TYPE OF ACCOUNT

Staff _____ Location _____

Faculty _____ Office No. _____

DEPARTMENT INFORMATION

Dept. Name _____

* DATES OF EMPLOYMENT

(Only for new personnel)

*START DATE:_____ * END DATE_____

ACCESS STATUS (Circle One)

Previous Access___ New Access___

Transfer to New Dept _____

*REQUESTED BANNER ACCESS (Check all that apply or write in)

□ Registration

□ Admissions

□ Major Changes

□ _____ □ _____

□ _____ □ _____

□ Event Management

□ Class Set Up

□ Advising

APPROVAL SIGNATURES

_____ _____

IMMEDIATE SUPERVISOR DATE

_____ _____

SENIOR DIRECTOR, ENROLLMENT SERVICES/REGISTRAR DATE

_____ _____

DEAN OF STUDENTS DATE

Information Technology Services

DATE COMPLETED:_____

COMPLETED BY:_____