Policy: Use of ISIS Data by Direct Access Users

The purpose of allowing direct access to information on or from ISIS (student information system) system is to provide management information including information to assist deans and vice chancellors in making data-driven decisions for their school/college or division. Direct access to ISIS data is not available for general use by faculty or staff. This policy addresses only the access privileges and handling procedures specific to ISIS data.

1. The data contained on ISIS are private and confidential. Authorization to use these data is given solely for job-related, educational purposes. Any use or disclosure of such information that is not permitted by state or federal law or University policy is strictly prohibited.

2. The Office of Institutional Research (OIR) remains the official source of academic management information (data, statistics) for the University. OIR will consult with departments, colleges, and other units on established definitions and data parameters to ensure the consistency of data generated for planning purposes. OIR will continue to be responsible for official enrollment, instructor, and course information for planning and program review purposes.

   Consistent with arrangements made with the OIR, any college, school, or functional offices in charge of inputting data should handle requests to them for such data/information, particularly requests made by individuals not affiliated with the University.

3. Recommending the granting of access to personnel within a school/college or division (but outside functional offices and the OIR) rests with the dean or vice chancellor. The dean or vice chancellor may recommend to the ISIS director a limited number of individuals to have the broad access given to Direct Access Users. ISIS information will only be accessed, transmitted or disseminated on a need-to-know basis by and for those individuals with a mission- and function-related need for the data for their unit. ISIS data forwarded in response to a report request should include a statement indicating that discretion should be used in further forwarding the information to other parties e.g., *The following report contains potentially sensitive data provided in response to a specific* need-to-know *request. Discretion should be used in forwarding this information to additional parties*.

4. Direct Access Users have access to university-wide data in ISIS, but are obligated to use only data specific to their needs. Sensitive data such as social security numbers, student grades and grade point averages, and student financial information will not be used except when essential to the project or as directed by authorized reporting agencies, and should always be handled with particular care. Where

possible, the University Personal Identification number (UID) will be used instead of the social security number. An example of unauthorized use of data would be for a college to generate mailings sent to admitted or prospective students who have not indicated an interest in that college, or mailings otherwise inconsistent with Office of Admissions policy.

5.   Under no circumstances may ISIS information be displayed, copied or e-mailed for purposes unrelated to the user's administrative duties or to individuals for personal knowledge or gain.   No employee of the University may generate lists of names from the ISIS database to distribute to an unauthorized third party for purposes apart from the mission of the University. An example of unacceptable distribution of ISIS data would be to provide a local business with the names and addresses of incoming students for advertising that business' products or services.

6.   Non-aggregate student data will not be stored outside of ISIS unless the storing of such data is necessary to the project or operations. Typically, non-aggregate student data will be stored in secure locations that are certified as secure by the Computing Services Security Team. If it is necessary to store these data on laptops or desktops, measures must be taken to secure the data including such measures as the following:

- the use of personal firewalls on the machines,
- hard drive encryption,
- security audits of such machines by Computing Services at least once a year.

7.   Direct Access Users are responsible for protecting all data consistent with University policy. Users are required to read and be familiar with this ISIS policy and the following areas of national and University policy and to sign the form at the bottom of this policy statement signifying their agreement to comply with all applicable policies in order to be given direct access to ISIS data. Examples of such policies iclude but are not limited to the following.

- GLBA, http://www.ftc.gov/privacy/glbact/glbsub1.htm
- Academic Policy 1900.10
  http://www.uark.edu/admin/vcacsey/AcaPolicySeries/190010.doc
- the Institutional Research Board's policies on human test subjects
  http://www.uark.edu/admin/rsspinfo/compliance/human-subjects/irb/IRB-Policy-Proc20020228.pdf
- The Code of Computing Practices
  http://compserv.uark.edu/policies/code.htm

Failure to comply with any provision of these policies may result in loss of access to ISIS data and/or disciplinary action, including the possibility of dismissal.

User Agreement

As a Direct Access User, I signify my recognition that the information contained on ISIS is private and confidential and that I am authorized to use this information solely for the job-related, educational purposes for which I have been approved. I understand that any use or disclosure of such information that is not permitted by state or federal law or University policy is strictly prohibited.

As a Direct Access User, I understand that compliance with these regulations and agreements will be reflected in my performance review, and that failure to comply will result in loss of access and in disciplinary action including the possibility of dismissal.

Direct Access User

_____Signature

_____
Printed Name

_____
Date

As the supervisor of this Direct Access User, I affirm that direct access is required for this employee position, consistent with the mission and function of the unit which I head and in which he or she is employed. I accept responsibility for use of access and any release of data by this user.

Administrative Director/Dean/Vice Chancellor

_____
Signature

_____
Printed Name

_____
Date

Office of the Provost, March 15, 2007