

FERPA, DATA MANAGEMENT AND DATA SECURITY POLICY	DOCUMENT NO.	
	Effective Date	
	Revision Date	January 21, 2003
	Revision No.	
	Page No.	1 of 5
	Approval:	

1.0 Purpose

This policy establishes guidelines for the management, use and security administration of institutional data that exists within the NAU reporting environments including, but not limited to the Data Warehouse, Operational Data Stores, Data Marts, and the PeopleSoft Transactional System.

This policy does not apply to other NAU transactional systems including, but not limited to Advantage and IDMS.

2.0 Revision History

3.0 Definitions

(These definitions are only in reference to data access under this policy)

**DATA ADMINISTRATION:** Comprised of the Data Trustees, the University Data Administrator and Data Stewards.

**DATA ADMINISTRATOR:** The University Data Administrator functions as the key liaison between technology professionals, Data Stewards, Data Trustees, and the user community to facilitate the use of institutional data, and to assist in the development of accessible, reliable and accurate data and information.

**DATA MART:** A Data Mart contains a subset of historical information from the Data Warehouse. Data Marts are focused on a particular subject area.

**DATA STEWARDS:** Those identified by a Data Trustee to manage a subset of data (i.e., they are responsible for its accuracy, integrity, and privacy).

**DATA TRUSTEES:** The most senior executive officers of the University or their designees.

**DATA USERS:** Employees of the University who access institutional data in the performance of their assigned duties.

**DATA VIEWS:** A collection of data elements, possibly from multiple databases, that are assembled and presented together.

FERPA, DATA MANAGEMENT AND DATA SECURITY POLICY	DOCUMENT NO.	
	Effective Date	
	Revision Date	July 2, 2002
	Revision No.	
	Page No.	2 of 5
	Approval:	

3.0 Definitions con't

**DATA WAREHOUSE:** A comprehensive and centralized database for storing institutional information. Allows the NAU community to assess past performance, develop better forecasts and support business decisions.

**ELIGIBLE EMPLOYEES:** Appointed personnel, including faculty and administrators, and staff, including temporary and student employees, and graduate assistants, of the University.

**FERPA:** The Family Educational Rights and Privacy Act of 1974 (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.

**INFORMATION RESOURCE MANAGEMENT:** Refers to the team responsible for the delivery of data and information to the University from NAU's Data Warehouse, Operational Data Store, and Data Marts. For further information, see the Information Resource Management Charter at <http://www4.nau.edu/pmo/irm/index.htm>.

**INFORMATION RESOURCE MANAGEMENT STEERING COMMITTEE:** Members of the NAU community that represent the Data Trustees and serve on the committee at their discretion. For further information, see the Information Resource Management Charter at [http://www4.nau.edu/pmo/irm/steering\\_committee.htm](http://www4.nau.edu/pmo/irm/steering_committee.htm).

**INSTITUTIONAL DATA:**

- Is relevant to collecting, planning, managing, or auditing an academic and/or administrative function of the University;
- Includes student, course, employee, university financial and campus community data and information; and
- Is included in official university administrative reporting.

**LIMITED-ACCESS DATA:** These are data elements and data views that, because of legal or ethical constraints or other clearly defined constraints such as personal privacy rights may not be accessed without specific authorization or to which only selective access may be granted.

**OPERATIONAL DATA STORE (ODS):** The component of the Data Warehouse that provides tactical support for the NAU community. It captures current operational data on a nightly basis.

FERPA, DATA MANAGEMENT AND DATA SECURITY POLICY	DOCUMENT NO.	
	Effective Date	
	Revision Date	July 2, 2002
	Revision No.	
	Page No.	3 of 5
	Approval:	

3.0 Definitions con't

RESEARCH DATA EXCLUSION: Applies to any unpublished information regarding any research done at or by the University, at any location, by faculty, staff and students in the course of teaching or research and not otherwise available to, or accessible by, third parties. These data include: notebooks, protocols, progress reports, final reports, drafts, funding requests, proposed budgets, contracts (public or private), computer generated and/or computer readable material, databases, codes, source codes or software.

TRANSACTIONAL SYSTEM: The operational system(s) from which the Data Warehouse extracts data, i.e. PeopleSoft HRSA and Advantage.

4.0 Persons Affected

- 4.1 All eligible employees who are in need of institutional data to complete their assigned duties.
- 4.2 Data Administration, including Data Trustees, the Data Administrator and Data Stewards, who are responsible for the integrity of institutional data and information as a part of their assigned duties.

5.0 Policy

This policy applies to institutional data only, as defined below, and is intended to improve access to these data by employees in the performance of their assigned duties. This policy does not apply to public access to these data nor does it apply to: (1) notes and records that are the personal property of individuals in the University community, or (2) materials as defined in the Research Data Exclusion definition. In all cases, applicable federal, state and local statutes and regulations that guarantee either protection or accessibility of institutional records will take precedence over this policy.

All eligible employees have access to institutional data for use in the performance of their assigned duties. As necessary, Data Administration may designate some data elements and data views as being limited-access data. Such designations must include the specific reference to the legal or ethical constraints or other clearly defined constraint, such as personal privacy rights, that requires this restriction. Such designations must also include a description of the categories of data users who are typically given access to the data, the conditions under which access is given or the limitation that applies to such access.

FERPA, DATA MANAGEMENT AND DATA SECURITY POLICY	DOCUMENT NO.	
	Effective Date	
	Revision Date	July 2, 2002
	Revision No.	
	Page No.	4 of 5
	Approval:	

5.0 Policy con't

Any data user may request that the appropriate Data Steward review the restrictions placed on a data element or data view. Data Administration makes final decisions on matters of data restriction and request for access rights to institutional data.

Any data user may request from Information Resource Management that additional institutional data reside within NAU's data warehouse. The Information Resource Management Steering Committee will review the request to determine its validity and priority.

Data users are expected to access institutional data only in the performance of their assigned duties, to respect the confidentiality and privacy of individuals whose records they access, to observe any ethical restrictions that apply to data to which they have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.

Expressly forbidden is the access or use of any institutional data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's own personal curiosity or that of others. Also forbidden is the disclosure or distribution of any institutional data in any medium, except as required by an employee's job responsibilities.

Violators are subject to disciplinary procedures of the University. In addition, restriction of access to data may result.

6.0 Responsibilities

- 6.1 Data Administration is responsible for defining and documenting procedures by which data users gain access to institutional and limited-access data.
- 6.2 An eligible employee who requests access to NAU's data warehouse will be granted access to institutional data upon the successful completion of the FERPA exam.
- 6.3 FERPA education will be required for all NAU employees. FERPA exam results will be recorded in a centralized database.

FERPA, DATA MANAGEMENT AND DATA SECURITY POLICY	DOCUMENT NO.	
	Effective Date	
	Revision Date	July 2, 2002
	Revision No.	
	Page No.	5 of 5
	Approval:	

6.0 Responsibilities cont.

- 6.4 The FERPA Review Team, consisting of representatives from Student Life, Registrar, Bursar, University Data Administrator and academic units, will be responsible for the content management and update of FERPA education.
- 6.5 Access to limited-access data will be granted to any employee who successfully completes the access form and obtains authorizing signatures from their direct supervisor and the appropriate Data Steward.
- 6.6 Information Resource Management will provide access to NAU's data warehouse environment upon verification that the employee successfully passed the FERPA exam and requested access.
- 6.7 Information Resource Management will provide access to limited-access data upon receiving the appropriate approved forms.
- 6.8 Information Resource Management Steering Committee is responsible for reviewing, approving and prioritizing all requests for additional institutional data inclusion within NAU's data warehouse.
- 6.9 Information Resource Management will administer the Business Objects© data access software, which includes security, environmental and document configurations.
- 6.10 Information Resource Management may remove access to institutional data upon termination of employment or violation of this policy.

7.0 Procedures

\*\*Procedures will be developed upon approval of this policy.