



NAU Data Access Policy

Philosophy

Data is one of the University's vital resources. University Data is the property of NAU and represents official University records. Data is independent of media on which it is stored or presented; it may be on-line, in a file, printed on paper, stored on micro-fiche, or on other media.

Security is required to protect the integrity of the University's data.

Employee access to data is a privilege granted for the express purpose of providing direct support of the University mission.

It is reasonable to attempt to meet the need to protect University data while still allowing employee access to that data.

Ethical Use of Data

Only actions which unquestionably conform to the purpose of providing direct support of the University mission are considered ethical use of University data. Any other access, representation, application or disposition of University data is considered unethical abuse of the privilege of access to data and may be cause for discipline, including dismissal, of employees and expulsion of students, as well as criminal prosecution.

Responsibilities of an Employee in the Use of University Data

Users who accept access to University data also accept responsibility for understanding:

- The meaning and purpose of the data.
- Controlling access to and release of data covered by law such as the Family Education Rights and Privacy act of 1974 (FERPA) governing confidentiality of students' educational records.
- Maintenance, storage and disposal of data in a secure, responsible and accountable manner.
- Verification that alternate representations of the data, such as ad hoc reports are indeed true and fair representation of the original data and are labeled 'unofficial'.
- Notifying the appropriate data steward before disseminating data to external agencies or entities [Note: the data steward may issue standing authorization to certain departments or individuals for release of information to external agencies.]
- Requesting assistance from the appropriate department for data requested or required by other internal entities.
- Reporting cases of abuse whenever and wherever they are encountered.



LOUIE Administrative Security Request

Current date:	Desired effective date for this request:	NAU UserID:
Name (Last, First, Middle Initial):		NAU Employee Id (not SSN):
Department:		
Job Title:		
Work Phone:		
Email Address (NAU accounts ONLY):		

SUPERVISORS: check here to remove all access from a user

Manager/Supervisor Name & Phone:
<input type="checkbox"/> I confirm that I have completed the FERPA tutorial located at http://www4.nau.edu/ferpa/ I understand that access will not be granted until this tutorial is complete. Initial here:

Business Need:

Please list the roles and action requested in the appropriate box below.

Add Security Roles	Remove Security Roles

As the employee requesting this access to the LOUIE system, I have read and agreed to abide by the NAU Data Access Policy which describes my responsibilities in the ethical use of the University's data.

Employee Signature:	Date:
----------------------------	--------------

As the supervisor of the employee requesting access to the LOUIE system I have confirmed the employee has completed the appropriate training for the access requested above.

Manager Signature:	Date:
---------------------------	--------------

Routing Instructions: Mail form providing all above information to LOUIE Security at Box 5200 or FAX to 928/523-0330

Signature of the Data Steward indicates that the access requested is appropriate for the specific job duties of this user

AD (Box 4084)	AI (Box 4128)	CC (Box 5200)
FA (Box 4108)	HR (Box 4113)	SC (Box 5100)
SF (Box 4079)	SR (Box 4103)	TX (Box 5200)

Data Steward signature is required for any role which provides access to data safeguarded by the Data Steward.	NAU Security Team Signature:	Date:
--	-------------------------------------	--------------



Guidelines for completing the LOUIE Administrative Security Request Form

Date: Today's Date

Desired effective date for this request: Provide desired completion date for this security request.

NAU Authentication ID: This is your NAU UserID. When you log on to NAU services, your UserID is required for NAU Authentication through NAU's Central Authentication System (CAS). If you are unsure of your id, call 3-1511.

Name: Enter your full name. Please do not use nicknames or alias's.

NAU Employee ID: The seven-digit number that can be found on the middle right hand section of your pay stub. This is NOT your Social Security Number.

Department: Your current department. This is the department that will be vouching that access to LOUIE is required to accomplish your job duties.

Job Title: Your current job title (e.g. Student Worker, Associate Professor, Administrative Associate).

Work Phone: The work phone where we can reach you.

Manager/Supervisor Name and Phone: Your supervisor's full name and office phone number. This information is required for your access to be approved.

Email Address: Your NAU email addresses.

FERPA requirement: In order to protect the confidentiality of educational records and students' rights to privacy, and in keeping with federal regulations and standard operating procedures at most national institutions of higher education in the US, NAU has adopted a policy that requires all employees who have access to the student information system to complete a tutorial on the Family Educational Rights and Privacy Act of 1974, FERPA. Failure to complete the required tutorial can mean the prevention or revocation of security access to the student information system.

Business Need: A brief explanation of the business requirement for the access (e.g. "to accomplish job duties assigned the payroll department" or "to advise students").

SUPERVISORS: If you want to have all access removed from an employee or former employee, check here, sign and date form.

Security Roles: This will grant the user a set of permissions. Check the New LOUIE reference sheet for guidelines on security roles.