University of Nebraska Lincoln

Request for access to UNL Identity Management services

Please read through the entire form before completing. You must complete a new form (separate request) for each project.
All needed signatures need to be obtained by the requester before final submission to the IDM Steering Committee.

LDAP is the Lightweight Directory Access Protocol. UNL uses LDAP as the primary directory service for authentication and directory lookups for UNL faculty, staff and students. Various levels of access to the directory can be established. This form is used to request access to the LDAP server.

Currently two different types of data access can be requested from the LDAP server. They are access to student data and access to HR data. Access to both student data and HR data can be simultaneous. For each type of access requested, approval must be obtained.

This form will be in effect for one year from the time it is processed. At that point it may be necessary to be re-authorized. You will be notified before your renewal time.

Use of the LDAP service/data for purposes other than those listed below will result in account revocation and may lead to disciplinary action, up to and including termination of my employment!

Technical contact:

Name:

Campus address, Zip:

Title:

Department:

Telephone:

Email:

Are you replacing a former user? ○ Yes ◉ No

If yes, person's name:

Administrative contact:

Name:

Campus address, Zip:

Title:

Department:

Telephone:

Email:

Are you replacing a former user? ○ Yes ○ No

If yes, person's name:

Server address:

Vendor Info:
(if applicable)

Application and/or purpose for access:

Please include as many details as possible to explain as much as you can about the frequency of data access, type of data needed, security of the application, length of time the data will be held, and any other details that may help the committee to understand the project.

Applicant authorization:

Dean's/Director's name:

Telephone:

Dean's/Director's signature:

Date:

Love Library, 4th Floor, Rm. 413: Attention IDM team / Lincoln, NE 68588-0496

(402) 472-7690 / FAX (402) 472-5280

Type of access:

- ☐ Direct access to LDAP
- ☐ Portal authentication via CAS
- ☐ Access for sponsored-guest users

Access to Student Data:

I need access to:

- ☐ All Students except those who have the privacy flag set
- ☐ All Students including those who have the privacy flag set (Approval required from UNL Registrar)

I need access to the following fields:

- ☐ Authentication only (Approval not required)
- ☐ Name/Address/Phone/College/Major/Class Standing (Approval not required)
- ☐ NCard NU ID Number (must not be publicly searchable, and should be used as user index)
- ☐ Email Address (Approval required from UNL Registrar)
- ☐ NCard ISO Number (Approval required from UNL Registrar)
- ☐ Student Fee Status (Approval required from UNL Registrar)
- ☐ Gender (Approval required from UNL Registrar)
- ☐ Birth date (Approval required from UNL Registrar)
- ☐ Student ID Photo (Approval required from UNL Registrar)

Registration and Records Approval, 59 Canfield:

Signature: _____ Date: _____

Comments/Restrictions:

_____

_____

_____

Access to Human Resources Data:

I need access to the following fields:

- ☐ Authentication only (Approval not required)
- ☐ Name/Address/Phone/Email/Title/Department (Approval not required)
- ☐ NCard NU ID Number (must not be publicly searchable, and should be used as user index)
- ☐ NCard ISO Number (Approval required from UNL Assistant Vice Chancellor for Human Resources)
- ☐ Personnel number (Approval required from UNL Assistant Vice Chancellor for Human Resources)
- ☐ Gender (Approval required from UNL Assistant Vice Chancellor for Human Resources)
- ☐ Birth date (Approval required from UNL Assistant Vice Chancellor for Human Resources)
- ☐ Employee ID Photo (Approval required from UNL Assistant Vice Chancellor for Human Resources)
- ☐ Employee home address (Approval required from UNL Assistant Vice Chancellor for Human Resources)

Assistant Vice Chancellor for Human Resources, 407 Canfield:

Signature: _____ Date: _____

Comments/Restrictions:

_____

Information Security and Application Scanning

(Signature required when access to non-public information is requested)

Information Security Admin, 211 Nebraska Hall:

Signature: _____ Date: _____

Comments/Restrictions:

_____

Statement of Understanding on the Use of Confidential Information

(To be completed only when access to non-public information is requested)

Individuals given access to confidential information regarding employees or students must understand and accept responsibility for maintaining the security and integrity of that information. The Federal Family Educational Rights and Privacy Act mandates that student information (other than that designated as public information) must be kept confidential. It further limits access to such information to that required to fulfill your institutional job responsibilities. The confidentially of employee records are similarly protected by federal and state statute as well as by institutional policy.

Your actions regarding the use of this information are governed by the policies stated in University of Nebraska Executive Memorandum 16 (Policy for Responsible Use of University Computers and Information Systems), Guidelines for the Use of Computing Resources at UNL and Executive Memorandum 26 (University of Nebraska Information Security Plan). By signing this Statement of Understanding you agree to abide by all current University policies regarding the handling and safekeeping of this confidential information. This includes the following specific requirements:

- **You will not disclose any confidential information to any other individual in any setting except to the extent necessary to carry out your assigned job functions.**
- **You will only access this information for legitimate University business and will not use this information for personal purposes.**
- **You will not share your user ID or password information with anyone, at any time, for any reason.**
- **You will take measures to safeguard this information by securing any printed reports, screen images or electronic files from the view or access of others who do not have a legitimate business reason to view the information. This requires you to take all measures needed to secure and safeguard any data transferred from the directory services database to another computer system.**
- **You will not remove confidential information in any form (printed or electronic) from your work site.**
- **You will notify your supervisor immediately if you believe that your user ID or password have been compromised or stolen.**
- **You will notify your supervisor or the computer operations center immediately if you have reason to believe that the security of the directory services database or the information that you derived from it has been compromised by an individual not authorized for access.**

Any unauthorized use or misuse of the confidential information you are being given access to is grounds for disciplinary action including termination.

I understand and acknowledge my responsibilities when accessing and using the confidential information to which I am being given access. I certify that I have read and understand Executive Memorandums 16 and 26 and will abide by those policies and the special provisions noted above.

Admin Signature: _____ Date: _____

Tech Signature: _____ Date: _____

Setup: *(for Information Services use only)*

Request Approved: ◯ Yes ◯ No

Date Approved: _____

Approving signature: _____

Revision 3.0, 2012-11-May