Duties of ConnectND Campus Access Control Officers for the Finance and/or HRMS Systems

This presentation is for ConnectND Campus Access Control Officers (CACOs) for the Finance and/or HRMS Systems.

Campus Access Control Officers are responsible for facilitating requests for access for faculty and staff.

A Role Access Process has been developed for Campus Access Control Officers. This process should be followed to determine appropriate access for individuals on your campus.

Role Access Process

- Campus employee wants access or a change in access to ConnectND Finance or HRMS.

- Campus employee submits request to their department head via email, for new access or to request additional access.

- Department head approves or does not approve access or additional access.
  - If not approving, department head notifies employee

- If approving:
  - Department head submits detailed email request along with the appropriate form (either NDUS-HECN-007 ConnectND Access Request for HRMS Form or NDUS-HECN-008 ConnectND Access Request for Finance Form) to Access Control Officer for
    - Finance System, or
• Campus Access Control Officer approves or does not approve access or additional access

• If not approving, Campus Access Control Officer notifies employee

• If approving:

• Campus Access Control Officer requests access through the Remedy System by entering a ticket at http://www.helpcenter.nodak.edu or by using the Remedy Client.

If using Remedy via the Web, the Campus Access Control Officer will enter ConnectND for the institution, their own name, phone number and email address. The details of the request should be stated as well, such as the system (HRMS or Finance), and what types of access is needed. Either a NDUS-HECN-007 ConnectND Access Request for HRMS Form or a NDUS-HECN-008 ConnectND Access for Finance Form must be attached for each user. Up to three requests may be attached. Please note: requests submitted using Remedy via the Web are not assigned directly to the ConnectND Security Group, therefore they may take longer to reach the ConnectND Security Group than those submitted using the Remedy Client.

If using the Remedy Client, the Access Control Officer will enter their own campus for the institution in the Customer Section, their own name, phone number and email address. The details of the request should be stated as well, such as the system (HRMS or Finance), and what types of access is needed. Either a NDUS-HECN-007 ConnectND Access Request for HRMS Form or a NDUS-HECN-008 ConnectND Access for Finance Form must be attached for each user. Up to three requests may be attached. Any other private information for the user(s) should be entered in the work log portion of the Remedy Ticket. Assign the ticket to ConnectND Security (see detailed instructions for the Remedy Client at www.und.edu/dept/connectndsecurity/CampusAccess.html)
The Remedy ticket will be assigned to the HECN ConnectND Security Group, who will make the approved change, note on the work log of the Remedy ticket, notify the employee, and resolve the ticket. The Access Control Officer will automatically be notified.

NDUS Helpdesk will close the ticket.

Finance System only – When notified by Remedy the Access Control Officer will complete setting up User Preferences for the user(s).

**IMPORTANT**

A student will not be allowed to have the role of Campus Access Control Officer or Campus Help Desk.

A student will not be allowed to use a user’s logon to perform duties of the Campus Access Control Officer or Campus Help Desk.

This rule must be enforced to ensure privacy. If a student had this access, he/she could obtain information about other students private information, either by running a query or by changing another student’s password, signing on as the student, and gaining access to the student’s information.

**Guidelines for Student Worker Access**

One or more specific UserID(s) can be created for student worker’s use at the request of a department head or supervisor. The UserID is generic in nature. The UserID is requested and issued with the understanding that the requestor (supervisor or department head) is ultimately responsible for the UserID.

The UserID is set up so that the requestor can sign on for a student and the student can perform duties as assigned. The UserID and password should be kept private, with only the requestor (supervisor or department head) knowing the UserID and password. A log should be kept and an entry made whenever a student uses the UserID. The password should be changed frequently, at least once a month.
This eliminates the problem of student turnover, and insures that data is not being displayed or manipulated by students when they are not in your offices.

* * * * * * * * * * * *

Forms to request access and the instructions for each form can be found on the NDUS-HECN Public Forms web site at:
http://www.und.edu/dept/connectndsecurity/Forms.html

Download the forms so they can be completed electronically.