CNU Account Management Procedures

Department: Systems and Support
Document ID: 04.01.02
Reviewed: June 2023
Created: 3/15/17

Introduction

The purpose of this procedure document is to cover requesting, authorizing, administrating, transferring, and terminating accounts in compliance with SEC 501. This document is maintained by the ITS Systems team.

Onboarding - Faculty/Adjunct Faculty

- Adjunct faculty are hired by the Deans and entered into CIPPS by the Payroll Department.
    - The Deans submit I-9 and the AP-14 form to payroll.
    - Payroll requires that the faculty ID number be created prior completing the full hiring process, which may require coordination with the Registrar to ensure the faculty has been assigned to a course.
    - Payroll emails hire reports to the ISO every 30 days for review by hire date. New users identified in this report will be assigned Information Security Awareness Training in scholar with thirty day requirements to complete training.
- Full-time faculty are entered into PMIS by the HR department.

    - Entry into PMIS/CIPPS does not directly impact CNU ITS onboarding process.
    - Note: Users entered into PMIS without email are not assigned to CNU in the Commonwealth Learning Management System.
- Office of the Registrar first assigns someone to teach a class in Banner: Account created in Banner form SPAIDEN, then Banner form SIAINST (assignment to a college/department and as "faculty"), then Banner form SSASECT (actual assignment to a CRN).
    - CNU ID is generated, along with the initial password value. The email is also defined based on firstname.lastname@cnu.edu in Banner (GOATPAD third party ID). Conflicts are handled on a case-by-case basis by the ITS Systems & Support team.
- The following day the AD (Active Directory) Account feed process runs daily at 5am and creates a CNU Connect/AD (Active Directory) account for the faculty member.
    - The user is added to the faculty group in Active Directory (based on F/S/E primary record type in Banner) and associated mailing lists (faculty@cnu.edu).
        - F = Faculty
    - The user is also added to Google, which creates their email account.
- Credential delivery - depending on faculty type, a paper form is completed and handed to the faculty member with their account information (CNU ID and initial password). The Assistant Registrar is responsible for completing the paper form.
    - Adjunct: The Executive Secretary Senior for each of the Dean's Offices delivers a printed copy of their credentials, collects the signed DHRM policy and is required to notify the ISO via email so the users can be added into Scholar for online training.
    - Full-time: The Executive Administrative Assistant in the Provost Office delivers credentials, and collects the signed DHRM policy via email. They are also required to notify the ISO via email so the users can be added into Scholar for online training.

- The thirty day clock on Information Security Awareness training will begin upon receipt of the monthly payroll report from the business office.

Onboarding - First Year and Transfer Students

- First Year Students
    - Admission staff enters the admit code (AT, GT, GI, TA, TF) in Banner form SAADCRV and then that triggers the learner record in Banner form SGASTDN. The CNU ID number is generated when the individual is entered into Banner as a student.
        - Once Admission Staff have gone through the step above, the initial password value is generated. The email is also defined based on firstname.lastname.2-digit admit year@cnu.edu (example - pat.smith.17@cnu.edu). Conflicts are handled on a case-by-case basis by ITS Systems & Support staff.

    - The following day the ITS AD (Active Directory) Account feed process runs daily at 5am and creates a CNU Connect/AD (Active Directory) account for the student.
        - The user is added to the student group in Active Directory (based on F/S/E primary rec type in Banner) and associated mailing lists (students@cnu.edu).
            - S = Student
        - The user is also added to Google, which creates their email account.
    - For first year students, the Office of the Registrar looks up the student ID number via the Banner form SAAADMS, prints out and distributes the student's credentials during Setting Sail, including their initial password. Access to this tool is restricted to approved administrators.
- Transfer Students
    - Transfer staff enters the admit code (TA, TF) in Banner form SAADCRV and then that triggers the learner record in Banner form SGASTDN.
        - CNU ID is generated, along with the initial password value. The email is also defined based on firstname.lastname.2-digit admit year@cnu.edu (example - pat.smith.17@cnu.edu). Conflicts are handled on a case-by-case basis by ITS Systems & Support staff.
    - The following day the ITS AD (Active Directory) Account feed process runs daily at 5am and creates a CNU Connect/AD (Active Directory) account for the student.
        - The user is added to the student group in Active Directory (based on F/S/E primary rec type in Banner) and associated mailing lists (students@cnu.edu).
            - S = Student
        - The user is also added to Google, which creates their email account.
    - The Office of the Registrar looks up/resets and provides the student with their CNU ID number, initial password value, and login instructions in their welcome packet.
- Re-admitted Students
    - Former or returning students need to contact ITS to reactivate their password through the standard password reset/recovery process.
- Graduate Students
    - Former CNU Students: Handled as Re-admitted Students (see above).
    - Newly Admitted Graduate Students: The Graduate Education Support Specialist enters the non-CNU person individual into Banner form SAAEAPS. Next, he/she verifies (associate person w ID) and use the Banner form SPAIDEN to check IDs and if no match is found, the Graduate Education Support Specialist clicks on “Create ID” in SPAIDEN. The Graduate Education Support Specialist then sends separate emails to the user with the User ID and temporary password. The temp password is generated via the CNU Connect (my.cnu.edu) gold bar.

CHRISTOPHER NEWPORT UNIVERSITY

Onboarding - Classified Employees/AP/AP-14 Employees

- HR notifies ITS via email when there is a new hire.
    - In addition, to avoid creating duplicates, HR provides the last 4 digits of the new hire's SSN to the IT Helpdesk and alumni status (if applicable).
    - ITS Systems & Support staff check to see if the user exists, and if not, creates the user in Banner.
        - CNU ID is generated, along with the initial password value. The email is also defined based on firstname.lastname@cnu.edu. Conflicts are handled on a case-by-case basis.
        - Specific ITS information can be found in the New Employee ID generation process document.
    - HR adds the user to the Commonwealth Learning Center system to ensure the individual receives agency-specific training.
- The following day the AD (Active Directory) Account feed process runs daily at 5am and creates a CNU Connect/AD (Active Directory) account for the employee.
    - The user is added to the employee group in Active Directory (based on F/S/E primary rec type in Banner) and associated mailing lists (employees@cnu.edu).
        - E = Employees
    - The user is also added to Google, which creates their email account. Alumni are given an additional email alias, when they become employees.
- If the employee starts before new hire orientation, the employee may request credentials from ITS when their supervisor creates a work order in the helpdesk system.
- If the employee's first day is the new hire orientation, ITS Systems & Support staff look up the employee ID and provide them to the IT staff member conducting the Information Security Training. The employees are provided their CNU ID number (if not already known) and initial password value after the Information Security Training session and are encouraged to change it immediately. The employee ID is communicated to each person on an individualized slip of paper.
- At employee orientation HR collects the signed DHRM policy.
- Employees will receive in person information security awareness training at HR new employee orientation.
- Role-Based security training will be assigned based on department and any additional security roles based on system assignments.

Onboarding and Account Creation - Privileged User Accounts

- Supervisor completes ITS Privileged Account Request Form on behalf of the employee. In the case of an auditor, a CNU employee must act as a sponsor, complete the form, and complete the process.
- Supervisor (or sponsor) creates a Help Desk Request including attaching approved ITS Privileged Account Request Form.
- A ticket is created in the Help Desk ticket system, and assigned to the ISO for approval.

- ISO will assign Role-Based Training (ITS Role Based Security Standard v.1) based on access request and notify supervisor and user of training requirement and completion date. Upon notification of successful completion, the ticket is then routed to Systems Team for the creation of the named account.
- The Systems Team will then update the ticket with named account information and ISO will notify the end user of approval, document and close the ticket.
- Privileged user accounts, i.e. System Administrator or service accounts will follow the standard security principles of "least privilege" and “separation of duties”. Accounts should not be granted any more privileges than those that are necessary for the functions the user will be performing and conform to the Account Management Standard (04.1.0).
- Privileged user accounts are included in annual account review performed and documented by the ISO.

Onboarding - AP-14 Employees

- The source department or responsible supervisor submits a request through the IT Helpdesk system documenting the need for a CNU Connect account and the user’s first name and last name.
    - The responsible supervisor must provide a signed copy of the DHRM 1.75 policy and schedule the individual for Information Security Training either at Human Resources or online through the Information Security Officer. Confirmation of online Information Security Awareness Training will be tracked by the ISO.
    - IT Services should set the expiration date on the account to correspond with the end of the contract/engagement (if applicable).

Onboarding - Others

- The source department or responsible supervisor submits a request through the IT Helpdesk system documenting the need for a CNU Connect account and the user’s first name and last name.
    - The responsible supervisor must provide a signed copy of the DHRM 1.75 policy and schedule the individual for Information Security Training either at Human Resources or online through the Information Security Officer. Confirmation of online Information Security Awareness Training will be tracked by the ISO.
    - IT Services should set the expiration date on the account to correspond with the end of the contract/engagement (if applicable).

Transfers

- The source department or responsible supervisor submits a request through the IT Helpdesk system documenting the need for a CNU Connect account and the user’s first name and last name.

CHRISTOPHER NEWPORT UNIVERSITY

Termination - Faculty

- The Provost's Administrative Assistant enters faculty who are not returning to teach classes into the ERS system for termination.
    - Emeritus faculty are noted as retirees and may retain some access.
- The Executive Secretary Senior for each of the Dean's Offices enters adjunct faculty who are not returning to teach classes into the ERS for termination. These accounts are subject to a yearly review by ITS.
    - College of Arts and Humanities
    - College of Natural and Behavioral Sciences
    - College of Social Sciences
    - Luter School of Business
- IT resource providers log into the ERS (Employee Resource System) via CNU Connect (my.cnu.edu) and collects the resources specified, which include, but are not limited to:
    - eVA
    - Banner
    - Door access
    - Active Directory (computer & network account)
    - CNU Connect/Email/G Suite
    - Local Administrator Account
    - Named Account
    - VPN User Account
- These accounts are subject to a yearly review by ITS.

Termination - Students

- Typically, students do not terminate and retain CNU Connect/Banner access indefinitely.
- Withdrawals - CNU does not terminate a student's Banner/CNU Connect if they are expelled or if they withdraw. If a student is academically dismissed he/she can still access their record, but due to restrictions imposed by the office of the Registrar, they cannot register for classes. If a student is judicially dismissed, CHECS puts a hold on the account, so the student cannot register. Other offices, including Parking Service and the Library, can put a hold on a student's account, preventing registration. Students must address the reason for the hold with the department that placed it.

Termination - Employees

- Assuming the Employee Separation Policy (#5080) has been followed, HR or the supervisor enters the separation date, which triggers an email to the resource providers to remove the relevant resources.
- IT Resource providers log into the ERS (Employee Resource System) via CNU Connect (my.cnu.edu) and collect the resources specified.
- The Manager of Systems and Database Operations checks ERS daily to see if any action is required, as a backup to the resource providers.

- The Associate Director for Systems and Support or the Manager of Systems and Database Operations will notify the Information Security Officer of any changes to named account status including transfer and/or termination upon receipt by submitting a Help Desk Ticket.
- Information Security Officer will verify account status and update Role-Based Security log as inactive with corresponding date and action, and forward ticket to Systems Team for deactivation.
- Systems Team will remove the named account upon notification of termination, update ticket and ISO will note actions completed and close the ticket.
- Chief Information Officer will notify the Information Security Officer of ITS Department personnel changes and/or when access requirements change or account review and/or modification is necessary.
- HR or the supervisor enters the separation date, which triggers an email to the resource providers to remove the relevant resources.
- IT resource providers log into the ERS (Employee Resource System) via CNU Connect (my.cnu.edu) and collects the resources specified, which include, but are not limited to:
    - eVA
    - Banner
    - Door access
    - Active Directory (computer & network account)
    - CNU Connect/Email/G Suite
    - Firewall Administrator Account
    - Local Administrator Account
    - Named Account
    - VPN User Account

Termination - Urgent

- Urgent terminations are handled at the direction of the Director for Human Resources and actions are documented via a helpdesk ticket.

Termination - Others

- The source department or responsible supervisor submits a request through the IT Helpdesk system to remove access for the user.
- These accounts are subject to a yearly review by ITS.

ITS ERS Responsibilities

- The ERS (Employee Resource System) is available via CNU Connect (my.cnu.edu).
- ITS resource providers receive email when they should take action on an individual, document, and add/remove access as necessary, per Christopher Newport University Employee Separation Policy #5080.
- ITS staff with ERS resources assigned are responsible to check ERS daily to see if any action is required.

References

- Policy: Unified Data Policy #6015
    - http://cnu.edu/public/
- Policy: Employee Separation and Clearance Policy #5080
    - http://cnu.edu/public/
- DHRM Policy: 1.75 – Use of Electronic Communications - https://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf
- http://cnu.edu/alumni/benefits/email/
- Standard: CNU Account Management Standard (04.1.0)

Review

Access control procedures will be reviewed on an annual basis.