Cheyney University Policy Number

Policy on:

|  |  |
| --- | --- |
| Approved by:  |   |
| History: | Issued |  Effective date |
|   | Revised | Policies superseded or modified |
|   | Additional History N/A |
| Related Policies: |  N/A |
| Additional References: |  |

A. Purpose: ***Access privileges of employees who are hiring in, transferring, or leaving the University are approved and immediately changed to reflect their new status.***

B. Scope: All employees who are hiring in, transferring, or leaving the University.

C. Definition(s): List of terms used in the document; defines unfamiliar terms that have a specialized meaning in the policy.

D. Policy and Procedure(s): The purpose of this document is to define the steps performed and procedures followed by the Cheyney Office of Information Technology and Human Resources when an employee joins or leaves the University. The Universities Joiners, Leavers and Position Change policy is driven by the New Hire, Separation and Position Change checklist document. This document is maintained by the HR department and lists the various tasks each department needs to accomplish in setting up, removing or changing account roles and privileges. Any access to software or modules specific the department will be determined by the department head.

Onboarding:

The HR representative will send an email to the OIT helpdesk mailbox. It will automatically generate and create a SNOW ticket. OIT staff will then review the ticket and make the necessary revisions to it so that all of the applicable persons are notified of their responsibilities due to the joiner’s accesses.

Leaving:

The HR representative will send an email to the OIT helpdesk mailbox. It will automatically generate and create a SNOW ticket. IT staff will then review the ticket and make the necessary revisions to it so that all of the applicable persons are notified of their responsibilities due to the leaver’s accesses. All of the fields on the form should be filled out in their entirety.

Temporary Leave:

When an employee leaves temporarily (due to medical, administrative, or other personal short term leave), the staff member or immediate manager should submit a ticket to the helpdesk notifying IT staff of when they should disable the account due to the leave. If a manager requires access to the leaver’s mailbox, including new incoming mail, next higher level manager and an HR approval is required. (i.e. requestor’s supervisor). The staff member should also be notified that access is being granted.

Transfers and Department Changes:

For Active Directory:

Currently, for distribution groups which hold certain group permissions in Active Directory, an employee who has changed positions can request to the distribution owner to be placed in the new distribution group. That owner will contact the previous owner and have that employees name removed from the previous group. The employee may also send an email to the helpdesk requesting to be added to the new distribution list. Helpdesk personnel will then contact distribution list owner to make sure that the employee can in fact be added. All applicable accesses will then be added or removed.

For System/Application Access:

An email is sent by the employee to the helpdesk requesting access to a specific system or application. A SNOW ticket is auto generated. The helpdesk personnel then adds the manager as a ‘Watcher’ onto the ticket to receive permission to grant the request, to receive what levels of access the individual should have and other applicable approvals. Depending on the system, a request may also need to be sent to multiple business owners for approvals. Permissions are usually mirrored off of other roles and responsibilities. Any associated forms must be filled out and approved before granting access

E. Enforcement:

**A university employee or student who violates this policy risks a range of sanctions imposed by relevant university disciplinary processes, ranging from denial of access to any or all information technology resources up to and including termination (for an employee) or dismissal (for a student). He or she also risks referral for prosecution under applicable local, state or federal laws.**