University Policy

Volume I1: Information Technology	**I1.01.2** **User Account and Access Management** **Interim Policy** **Effective Date:** 06/30/2022 **Last Revised:** mm/dd/yy	**Responsible Office:** University Technology Services
Chapter 01: Acceptable Use		**Responsible Officer:** Information Security Officer

POLICY STATEMENT

User accounts provide the first line of defense against unauthorized access and activities that could compromise the confidentiality, integrity and availability of the University's critical information and operations.

It is important to establish a policy and procedure for appropriate management of user accounts to minimize the risk of unauthorized access to university information and IT resources and to promote adherence to federal, state and local, legal, regulatory, and statutory requirements (e.g., FERPA, GLBA, HIPAA).

PURPOSE OF THE POLICY

The purpose of this policy is to set out the requirements for user account provisioning and de-provisioning, access management and appropriate use of user accounts to protect the university's information and IT resources from unauthorized access or use.

WHO IS AFFECTED BY THIS POLICY

All users of university information and Information Technology Resources (ITR)

DEFINITIONS

Active Student: a person who is enrolled in classes at NEIU and who has attempted hours within the last 36 months or is a person who has been admitted to NEIU within the past 36 months, or who has been given an approved override by the Registrar's Office.

Registered Student: a person who is registered to take a class during the current semester, who has an incomplete grade that hasn't expired and whose Banner record is inactive, or who has been given an approved override by the Registrar's Office.

User Account: is a combination of a unique Network Identifier and password for accessing the University's email system and other IT resources.

Email: electronic mail. An information vehicle for communications within the University and between the University community and others worldwide, which provides communications and collaboration, reliability, security, and business continuity.

Separation: any faculty, staff, student, or contractor whose employment, academic studies, or any services performed for or on behalf of the University ceases.

Alumni: graduated students and former staff and faculty.

Affiliates: an individual working for the University who is not a payroll employee (e.g., a consultant)

Privileged Access: access for roles with application or system administrative responsibilities to be able to carry out operational management of the systems or applications they support.

Active User Account: the account is active and accessible to an individual.

Account Deactivation: the Account is no longer active and accessible to an individual but the account has not been deleted. This means that access is de-provisioned to the user.

Account Deletion: the Account is deleted from the University's system including email, Google Drive, and other contents held by the individual.

REGULATIONS

Students and Employees

Upon joining the University, a student or an employee will be provided with the standard user account. This is a unique Network ID and password.

When a student or an employee no longer has an active role at the University, based on notification from the source systems (e.g., HR, Academic Affairs Services, Enrollment Services systems), their user account will be deactivated following the requirements stated below.

Staff Employees

- Following a separation from employment, the user account will be deactivated immediately.
- Access to third-party managed systems must be deactivated. Line managers are responsible for ensuring the access is removed.
- University Technology Services will liaise with the relevant department to provide access to the email to a designee for work continuity purposes.

Note: Access for employees retiring from the University is covered under the Retiree section of this policy.

Faculty Employees

- For faculty employees leaving active job status, their user accounts will remain active for twelve (12) months following the end of the current contract. This is to maintain access to the employee should they return within the 12 months.
- Twelve (12) months after the end of an existing contract, a faculty employee user account will be deactivated.
- Dual Roles (staff and faculty): For faculty employees whose staff roles cease, the user account will remain active to support their faculty role but access to IT resources for their staff roles will cease.
- Following a non-voluntary separation, the user account will be deactivated immediately.
- University Technology Services will liaise with the relevant department to provide access to the email to a designee for work continuity purposes.
- LMS
- Upon request and approval by the department chair, dean and provost, the CTL will work with the departed faculty member, within reason, to provide course materials and data, as appropriate, from previous courses, not including personally identifiable information.

Students

- A university user account will be deactivated when a student ceases to be an active student.
- A university user account will be deactivated immediately for involuntary separation from the University.
- Requests for past coursework or related information may be provided (to the extent possible) to students upon approval by the department chair in compliance with applicable regulations.

Student Alumni: Access to email and Neiuport will remain eighteen (18) months after graduation or official completion of the academic program after which access will be deactivated.

Alumni: Returning alumni officially enrolled with the University will have their user account active for as long as they are in good standing or until the completion of their degree.

Additional Access: Access to additional information and IT resources (including third-party managed systems) may be granted to an employee based on their job function following authorization by the line manager. Line managers are responsible for ensuring access is reviewed periodically and access is removed when an employee leaves or changes their job role.

Shared Mailbox: Shared mailboxes provide access to multiple users to facilitate shared responsibilities and the use of shared resources. Mailboxes should have named owners. Passwords to shared mailboxes will not be provided to team members, rather users will be able to access shared mailboxes via delegated access from their inboxes. Passwords may only be provided to the named owner if it is needed for specific reasons. Passwords must not be shared.

Departmental Network File Drives: Access may be given to employees in other departments to the network file drives/other information resources of another department for cross-functional work and collaboration. Access requests must be authorized by the functional/project lead of the network file drive/information resources and must be removed after completion of work or when no longer required.

Shared Folders in Google Drive: Google Drive owners can give access to other users as deemed necessary for work. Drive owners are responsible for ensuring that access is removed when no longer required.

Line managers must ensure that employees separating from the University transfer ownership of shared folders and files in their Google Drive to other team members as deemed necessary to ensure continued access to these resources after the employee separates from the University.

Privileged Access: A privileged account must only be given to individuals with system and application administrator roles within the UTS (University Technology Services). It must be formally requested by the line manager and approved by the CIO before it is assigned to an individual. It must have a unique username and password. Line managers are responsible for ensuring privileged access is required for the job function before requesting access, and for requesting access deactivation when an employee separates from the University or changes their job role. Privileged accounts will be logged and reviewed periodically.

An IT system default administrator username and password must be changed before the system goes into production.

Elevated Access for Non-System/Application Administrators: Individuals or departments requiring elevated access permissions to computer systems/applications to support their job functions are to make a formal request to the UTS. The request must be authorized by the relevant line manager/supervisor with

the business need stated in the request. UTS will review such requests to determine the appropriate permission level required and will provide access accordingly.

For third-party managed IT systems and applications, functional leads are to ensure that privileged or elevated access permissions are provided according to the business requirements. Access should be logged and reviewed periodically.

Wireless Access: Access to the secure and unsecure wireless network will be available to use by students and employees. Employees should not use the unsecured wireless network for carrying out any work activity that uses confidential or sensitive work information.

Microsoft O365 Access: Access to the university's Microsoft O365 may be made available to students, faculty, and staff. Sensitive or confidential work information may not be stored in O365. The network file drives and Google drive are the approved storage areas.

Role Change: Line managers must ensure that access to IT systems for team members changing roles is reviewed in line with the new access requirements.

Affiliates: An affiliate may be provided with the standard user account depending on the business need. In cases where a different access type is required for a specific work (e.g., for technical system support), access will be granted as appropriate for the job. Access must have a timeframe assigned to it and must be reviewed periodically at least every 6 months.

Extension of Access After Employment: Access to university information and IT resources may be extended after the employment ends in cases where access is needed for ongoing projects or extended support from the departing employee.

Guests: The University's unsecure public network is available to guests. Guest access to the secure network is not permitted.

Retirees: Access to IT resources will be removed but access to the email account will be maintained. Historic email messages will be purged from the email account to ensure adherence to legislative requirements. University Technology Services will liaise with the relevant department to ensure that historic email is available to relevant designees for work continuity purposes.

Access will be deactivated to a retiree email account if the account has not been active in 3 years.

Deceased: Upon notification by the family of a deceased employee, the UTS will deactivate the employee's access and will work with Human Resources and the employee's manager to provide delegated access to the email to a designee for work purposes if necessary. The delegated access to the inbox will be removed upon notification by the manager.

Upon notification by the family of a deceased student, the UTS will deactivate the student's access. To support inquiries by the family of the student, UTS will work with Enrollment Services and the Registrar to make access to the student's user account available to the relevant designee within the faculty.

Creation and Use of University User Accounts

The Acceptable Use of Information Technology Resources is the overarching policy that governs the use of all university IT Resources including user accounts. User accounts must be created and used as follows:

- User accounts are only to be created and operated according to the requirements of this policy and are only to remain active for the period required to fulfill work or academic needs.

- Users must change the default password assigned to their accounts at first login.
- Users must use multifactor authentication where enabled.
- Account login details must not be shared with others. An individual's user account must not be used as a generic/multi-user account.
- Attempting to use accounts to gain access to IT resources and information that have not been authorized is prohibited.
- Attempting to escalate access privileges is prohibited.
- A privileged account must be operated solely for the intended purposes and separately from the standard user account.

Suspension of a User Account

A user account will only be suspended when continued use of the account could expose the University to events that could compromise the security of its information and IT resources or cause legislative or legal liabilities to the University or harm its image.

An account suspension must be authorized by the relevant representative from the faculty or administrative office involved in the investigatory process. The Human Resources Department will work with the department to ensure all relevant policies and processes are complied with. Suspension of a student account must be authorized by the dean of the college or nominated representative of the faculty.

Account Deletion

All user accounts will be deleted twenty-four (24) months after access is deactivated.

Enforcement

The University reserves the right to revoke a user account at any time. Any user of the University's information and ITR who violates the Information Technology/Security Policies and Procedures may be subject to disciplinary action, which may include removal or restriction of access to prevent any compromise of or damage to university information and ITR, or to protect the University from liability. Unauthorized access or disclosure of information protected by legislation (such as FERPA, IPA, HIPAA, etc.) may result in civil liability or criminal prosecution, and dismissal from the University.

PROCEDURES

Provisioning

- The identity management system (IDM) will create a user account when an employment or student record is received from the source system.
- Line managers and user account owners will be notified when an account has been created.
- Users are to change their default login passwords at first login via identity.neiu.edu.

Deprovisioning

- The identity management system will deactivate access to a user account upon receiving a notification of the end of employment, contract, or study status from the source system.
- Where an account is deactivated and there is a business need to activate the account, the relevant source system will trigger a notification to the IDM system for the account reactivation and afterward, a deactivation when it is no longer needed.

GUIDELINES

Information Security Standards
Cybersecurity Tips

HISTORY

Draft created June 2022

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Acceptable Use of Information Technology Resources
815 ILCS 530/ Personal Information Protection Act
Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102
Health Insurance Portability and Accountability Act (HIPAA), P.L. 104-191
5 ILCS 179/ Identity Protection Act
Illinois Social Security Number Protection Task Force Report
Family Educational Rights and Privacy Act, 20 U.S.C. §1232

CONTACT INFORMATION

Please direct questions or concerns about this policy to

Contact	Phone	Email
University Technology Services	*(773) 442-4357*	*help@neiu.edu*

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.