University Policy

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).

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.

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

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,

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.