THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

NETWORK, COMPUTER, AND EMAIL ACCOUNT ADMINISTRATION

INTERIM

Number 06.01.05

Division Administration - Office of Information Technology (OIT)

Date August 1, 2015; Revised July 20, 2018; Reviewed/Revised April 21, 2025

Purpose The purpose of this policy is to ensure creation and management of The University of Alabama in Huntsville ("UAH" or "University") network, computer, and email accounts in accordance with industry-standard best practices.

Policy This policy establishes the criteria and practices to ensure creation and management of network, computer, and email accounts in accordance with industry-standard best practices. In addition, this policy directs users, wherever possible, to utilize the university-wide trusted identity management source for creation, management, and removal of accounts**.**

In today's world of global communications, network, computer, and email accounts represent, both internally and to the outside world, an official affiliation with the university that carries with it certain obligations. Network, computer, and email accounts are also essential to protect resources and data, including data protected by Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR) and other regulatory requirements. These accounts may also represent intellectual property and/or economic interests of the university.

This policy applies to all IT usage by faculty, staff, students, affiliates, researchers, or other users of information technology (IT) resources that connect to UAH networks.

All usage of the term accounts in this policy is in reference to network, computer and email accounts.

1.0 University-wide Trusted Identity Management System

The university-wide trusted identity management system shall be the source for creation, management, removal of accounts and authentication of credentials, and is to be used for all UAH authentication. If it is not possible to utilize the university-wide trusted identity management system, the reasons are to be

documented and approved in writing by the unit head and campus Chief Information Officer (CIO) or the CIO's designee.

All business related to faculty and staff duties at the university must be conducted using a provided UAH email address. The use of non-UAH email addresses such as GMail to conduct official business is strictly prohibited.

UAH reserves the right to monitor account usage to ensure compliance with this and all other policies.

2.0 Account Eligibility

Each eligible individual obtaining an account will have a university-wide unique username assigned, built from a standard format following the university's ChargerID naming convention. All necessary steps will be taken to coordinate the assignment of ChargerID among all technical operations within the university where naming takes place.

All accounts will be directly assigned to single individuals based on eligibility rules, and those individuals will be the sole contact and have sole responsibility for all actions taken with and by that account.

All account holders will read and agree to a set of responsibilities regarding account access.

Individuals may have multiple accounts assigned to them. Requests for such accounts must be reviewed by the UAH CIO or the CIO's designee and the reason for them must be consistent with activities related to UAH functions.

System and service accounts such as, but not limited to, administrator, root, sys and any other account that is utilized to run a service are not governed by this eligibility requirements but are to be protected in accordance with the Security of IT Resources Policy and OIT security standards.

2.1 Account Authenticators

Account authenticators, such as passwords, passphrases, or multifactor authenticators are unique to individuals. No agent of UAH will ever ask for or require a user to give them their password for any reason. Only the account owner will know the account authenticators for accounts assigned to them. Circumstances under which IT support or system administrators or any other person can learn or obtain the user's account authenticators must be minimal in the extreme, and where possible initially assigned account authenticators must expire causing the user to choose a new one that only they know or have.

All systems containing UAH data or connected to UAH networks which use passwords or passphrases as authenticators in whole or part must support the following control mechanisms where technically feasible:

- Authentication using multi-factor authentication
- Minimum password length
- Lockout after a certain number of failed login attempts
- Maximum password age
- Prevent password reuse
- Enforce password complexity
- Logging of all successful and failed password changes and logon attempts and retain such logs for a minimum of 90 days
- Encrypted while stored or transmitted using algorithms approved by the UAH CIO or the CIO's designee
- Detection of unused accounts

UAH information systems that cannot meet the above requirements should be documented and sent to the CIO or the CIO's designee for review and approval.

If there is suspicion or confirmation that a user's authenticator has been compromised, the user shall be required to change the account's authenticator immediately.

Use of single factor biometric authenticators should not be utilized on devices that store sensitive or confidential data as defined in the Protection of Data policy.

Where multifactor authentication is utilized, all passwords follow the same requirements for length, lockout, history, complexity, logging and encryption, but are only required to expire every 365 days.

The user shall change the account's password / passphrase for access to UAH resources immediately, if there is a concern that the password / passphrase has been compromised.

3.0 Account Name Changes

ChargerID changes will be allowed where the combinations of characters result in an objectionable name or term. Vanity username changes will not be permitted.

4.0 Account Expiration and Privilege Revocation

Individuals may leave the university for a variety of reasons, including without limitation to take other employment, retire, transfer to another college, or simply go on to other activities.

For all accounts, all non-email account privileges will be revoked at the time of separation.

For all account types UAH reserves the right to revoke account privileges at any time for any lawful reason in UAH's sole discretion. For example, revocation may

be required because of individuals discontinuing their affiliations with UAH, known or suspected account abuse, legal request, known or suspected account compromise, or other reasons.

Email accounts will be removed in accordance with the details below:

Faculty - For faculty who voluntarily separate from the university, access to email accounts will be removed 120 days after separation. Faculty with a legitimate email access business need that may affect University operations may request continued access for a specific time period. This request must be approved in advance by the Provost and Executive Vice President of Academic Affairs or their designee and may not be for a period of more than 6 months following the former faculty member's separation from the university without approval from the UAH CIO or the CIO's designee.

Staff -- For staff who voluntarily separate from the university, access to email accounts will be removed as soon as possible after separation.

Students – Students who leave the university may keep their email account for three terms from the last term in which they were registered. All other account privileges will be revoked at the time of separation from the university.

Prospective students who have been given email privileges – Students who have been admitted to the university, but fail to register for classes in the term of their admission, will have their account privileges terminated immediately after census date for that first term has passed.

An employee who is terminated or a student who is expelled – Faculty, staff, or students who leave the university involuntarily will have all account privileges terminated immediately upon receipt of notification by Human Resources or the Dean of Students Office respectively.

Affiliates who have been granted email privileges – Affiliates are contractors, long-term guests and tenants, with a university sponsor, who have been granted account privileges. Affiliates will have all account privileges terminated effective on their last day of affiliation with the university as indicated by their sponsor.

Affiliate sponsors must be current UAH faculty or staff.

Affiliate accounts expire 90 days after creation unless a later expiration is agreed upon at time of creation (with a maximum of 365 days). All affiliate accounts must be reverified by the sponsor before the expiration period is set.

4.1 Account Expiration Exceptions

Exceptions to account expiration may be made by providing approval from unit head and next level supervisor, timeframe needed, and justification for exception.

Documentation should be provided to UAH CIO, or the CIO's designee, to approve the exception and maintain record.

5.0 Affiliate Accounts

Accounts may be assigned to individuals who are not current faculty, staff, or students of UAH only in support of activities directly associated with UAH functions. A current full-time faculty or staff member must identify himself or herself as the sponsor or contact related to the individual's activities while the affiliate is at the university. When requesting or renewing the account, this sponsor will provide information stating their relationship to the individual, outlining the individual's affiliation/benefit to UAH, and an indication that they understand their responsibilities related to the use of the individual account.

The UAH Office of Information Technology will make the initial determination regarding eligibility of an individual to receive a UAH account. Cases where eligibility is unclear will be passed to the UAH CIO or the CIO's designee for review and approval.

6.0 Account Information

Extracts of student, staff, or faculty information in support of account administration activities or user directories will be taken from official university sources.

Extracts of faculty/staff or student information in support of accounts administration activities or user directories will be used only for this purpose. Secondary release of this information is not permitted without review and approval by the UAH CIO or the CIO's designee.

7.0 Compliance with Policy

OIT personnel may take immediate action to abate identified issues impacting network or system operations.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, the Staff Handbook, or University policy, will be referred to appropriate university authorities.

Review The IT Investment Advisory Council is responsible for the review of this policy every five (5) years (or whenever circumstances require).