THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

NETWORK, COMPUTER, AND E-MAIL ACCOUNT ADMINISTRATION

Number 06.01.05

Division Finance and Administration - Office of Information Technology (OIT)

Date June 2018

Purpose The purpose of this policy is to ensure creation and management of network, computer, and e-mail 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 e-mail 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 e-mail accounts represent, both internally and to the outside world, an official affiliation with the university that carries with it certain obligations. Network, computer, and e-mail 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, researchers, or other users of information technology (IT) resources that connect to The University of Alabama in Huntsville (UAH) networks.

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

Procedure

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 Security Officer (CISO).

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 in that account.

All account holders will read and agree to a set of responsibilities before they gain control of their account.

Individuals may have multiple accounts assigned to them. Requests for such accounts must be reviewed 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.

2.1 Account Authenticators

Account authenticators, such as passwords, passphrases, or multifactor authenticators are unique to individuals, and Accounts or System Administrators, supervisors, or any other agent of UAH will never 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 Accounts 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.

When passwords or passphrases are used as the sole account authenticator, the following policies shall be applied:

1. Length: All account passwords / passphrases shall be a minimum of 8 characters in length.
2. Lockout: After 6 failed login attempts accounts shall be disabled and locked out for at least 30 minutes.
3. Expiration: Passwords / passphrases shall expire every 180 days or less.
4. History: Password / passphrase history shall be kept to prevent at least the previous six (6) passwords / passphrases from re-use.
5. Complexity: Passwords / passphrases shall contain at least 1 character from three of the following ASCII character sets: lowercase alphabetic, uppercase alphabetic, number, and symbols.
6. Logging: Systems shall log successful and failed logon attempts and retain such logs for a minimum of 90 calendar days.
7. Encryption: All credential usage shall be encrypted while in transit and storage.

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

UAH reserves the right to revoke all account privileges at any time. Revocation may be required because of individuals discontinuing their affiliations with UAH, account abuse, legal request, or account compromise.

Individuals may leave the university to take other employment, retire, transfer to another college, or simply go on to other activities. Account benefits are reduced depending on the following roles. The normal expiration of accounts will be determined as follows:

Faculty who leave before retirement – Faculty members who leave the university before retirement may keep their e-mail account for one year from the end of the last term in which they taught. All other account privileges will be revoked at the time of separation.

Staff who leave before retirement – Staff members who leave the University before retirement will have all account privileges terminated effective on their last work day as determined by Human Resources, unless specific arrangements are requested and approved by Human Resources.

Retired Faculty, Retired Staff and Emeritus Faculty – Faculty and staff members retiring from the university or obtaining Emeritus status may elect to retain their UAH e-mail privileges. Upon transitioning from full-time to retired status, retired faculty and staff may be asked to sign an acceptable use agreement. For security reasons, if there is no usage for a period of one year, e-mail privileges may be terminated. All other account privileges will be revoked at the time of separation.

Adjunct Faculty – Adjunct Faculty members may maintain e-mail privileges for one academic year from the last term in which they taught. All other account privileges will be revoked at the time of separation.

Students who leave before graduation – Students who leave the university may keep their e-mail 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.

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

Alumni – Alumni may retain e-mail privileges on their primary account for one year (or three terms) after graduation. Alumni will be provided an alumni account shortly after graduation for their continued use. Alumni who would like to request an account may register for e-mail privileges by going to the Alumni Website (http://www.uah.edu/alumni). All other account privileges will be revoked at the time of separation.

An employee who is terminated or a student who is expelled – Employees 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 e-mail privileges – Contractors, long-term guests and tenants, with a university sponsor, who have been granted account privileges will have all account privileges terminated effective on their last day of affiliation with the university as indicated by their sponsor.

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 direct reports, to approve the exception and maintain record.

5.0 Guest Accounts

Accounts may be assigned to individuals not affiliated with 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 they are 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.

UAH Helpdesk 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 campus CISO for review and approval.

UAH Helpdesk will retain all documentation related to accounts while the account is active, and for one year following the point at which the individual is no longer associated with UAH, or from the point where the organization having a group account has been dissolved.

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 campus CISO, and the data owner associated with the data involved.

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 years (or whenever circumstances require).