AUBURN UNIVERSITY
AT MONTGOMERY

Account Retention Policy

Effective:
Prior Versions:
Responsible Office: Information Technology Services (ITS)
Review By:

I. Purpose

Auburn University at Montgomery (AUM) provides users access to its technology resources via accounts. The purpose of this policy is to ensure consistent account retention practices.

II. Policy

User accounts are available to AUM students, faculty, staff, vendors and guests. When a student graduates from the University or is otherwise no longer enrolled, or an employee leaves the University, his or her user account is available for a period of time as determined by the Account Retention Policy and then the contents are purged. Purging an account consists of permanent deletion of email and other stored data. Guest accounts are temporarily granted to vendors, trainers, visitors, and guests of the University.

III. Applicability

This policy applies to all University faculty, employees, students, vendors, and guests.

IV. Definitions

Account Deactivation - consists of disabling an account. Email continues to collect. Email, network drives, and other stored data remain, but the user is unable to access these resources.

Account Purge - consists of permanent deletion of email, network drives, and other stored data.

V. Procedures

Students

- Students who graduated may retain their current email for one (1) year and will be deactivated thereafter.
- Students who do not re-enroll and did not graduate will be deactivated after 3 terms (Spring, Summer, and Fall) of not attending classes.
- Deactivated student accounts are purged sixty (60) days after the deactivation date.
- Students are sent an email regarding deactivation approximately thirty (30) days before deactivation.

Employees

- The accounts of staff are deactivated upon separation date or last work date.
- The accounts of retired faculty and staff will remain active with email access in accordance with AUM's email policy and Document Retention Policy.
- Due to their dynamic nature, the accounts of Faculty and Temporary Faculty who have separated, are audited and evaluated once a year by the Office of the Provost and may be deactivated if deemed to no longer be needed.
- Access to the former employee's network drive, email, computer, and other systems is available upon the supervisor's request if a valid business reason exists that is aligned with the Acceptable Use Policy. This request is made to Human Resources and coordinated with Information Technology Services.

Other Accounts

- AUM may provide accounts in Active Directory for vendors, trainers, and guests of University employees.
- Wireless guest accounts with Internet-only access are available for University visitors in accordance with the AUM Wireless Policy. These accounts must not have access to confidential information unless deemed a business necessity by the University. They are only to remain active for a predetermined period established by AUM.
- All other accounts including but not limited to auxiliary employees, vendors, as well as community members are subject to closure without notice after the person's affiliation with the university is concluded. Since these accounts are used for university business, access to those accounts may be restricted immediately upon completion of service.

General

- Data and email cannot be recovered once an account is purged.
- The University may, within its discretion and notwithstanding the timeframes above, deactivate inactive accounts. An inactive account is an account that does not log-in or check email.
- Special Accounts (including Student Worker, Graduate Assistance, Club, Departmental, and Guest Accounts) must have an AUM sponsor and point of contact.
- It is the responsibility of the account holder to ensure they have copies of any desired data such as email, contacts, or user files before the deactivation of their account.

VI. Sanctions

Violations of this policy may result in actions ranging from warnings to loss of access to AUM IT resources.

Employee violations of this policy or the protection standards created to implement this policy may also be considered a Group I infraction under the University Personnel Manual and subject to disciplinary action, up to and including dismissal.

VII. Exclusions

NONE

X. Interpretation

Questions about the interpretation of this policy should be directed to the Office of the Chancellor.

SIGNATURE: _____ DATE: _____