
Purpose:

To establish requirements for account and access management, including creation, approval, authorization and termination.

Standard:

1. Each user of an Information System will be issued a unique account and identifier (username) for an Information System. Whenever possible, Information Systems should utilize Gatorlink accounts, otherwise unique identifiers should match those of the enterprise-issued account assigned to the user. Unique identifiers will not be reissued to anyone other than the original user. Systems in which it is not possible to assign unique identifiers to each user must implement compensating controls to limit access and provide accountability.
2. Units must document approval to issue each account, the type of account (individual, group, system, guest/anonymous and temporary) and the scope and level of access assigned to that account. This documentation must be maintained for a minimum of XXX.
3. Authorizations must only grant the minimum level of access to University Data and Information Systems needed to perform the intended function.
4. Every account on an Information System must be reviewed prior to being placed into use and annually thereafter. The approval and authorizations for each account must be verified.
5. Accounts not used within 180 days are to be disabled, and must be explicitly re-enabled prior to further use. Temporary accounts should be issued with a pre-set expiration date.
6. Accounts and authorizations must be promptly modified when the assigned user's job duties or assignment change, or upon termination of employment. Managers should coordinate with appropriate staff to ensure immediate suspension of accounts assigned to employees that are involuntarily terminated. Access methods (such as passwords) for any shared accounts must be changed upon termination of an employee with use of the shared account. Temporary and Guest access must be monitored and promptly suspended or removed once authorization expires.

Standard: Account Management



References:

DRAFT

Standard Number:
SEC-AC-nnn.nn

Standard Family:
Information Security

Category:
Access Control

Effective Date:
xx/xx/201x