AC-2 Account Management

Description

Access to University information resources is commonly controlled by a logon ID associated with an authorized account. Proper administration of these access controls (e.g. logon IDs and passwords) is important to ensure the integrity of university information and the normal business operation of University managed and administered information resources.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources data/owners, management personnel, and system administrators.

Implementation

1. An approval process is required prior to granting access authorization for an information resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use (Information Technology related Rules and SAPs such as University Rule 29.01.03.M2 Rules for Responsible Computing) and the granting of authorization by the resource owner or their designee.

2. Each person is to have a unique logon ID and associated account for accountability purposes. Role accounts (e.g., guest or visitor) are to be used in very limited situations, and must provide individual accountability.

3. Access authorization controls are to be modified appropriately as an account holder's employment or job responsibilities change.

4. Account creation processes are required to ensure that only authorized individuals receive access to information resources.

5. Processes are required to disable logon IDs that are associated with individuals that are no longer employed by, or associated with, the University. In the event that the access privilege is to remain active, the department (e.g., owner, department head) shall document that a benefit to the University exists.

6. All new logon IDs that have not been accessed within a reasonable period of time from the date of creation will be disabled.

7. All logon IDs having access to mission critical and/or confidential resources that have not been used/accessed within a period of six months, shall be disabled. Exceptions can be made where there is an established departmental procedure. These actions shall be reviewed and

approved by the department head or director. Documentation shall be maintained by the system administrator or other designated responsible official.

8. Passwords associated with logon IDs shall comply with Control IA-5 Authenticator Management.

9. System Administrators or other designated staff:

    9.1. Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to TAMU information resource.

    9.2. Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.

    9.3. Shall have a documented process for periodically reviewing existing accounts for validity.

Last Revised September 1, 2016

(This control replaces previous SAP 29.01.03.M1.03 Information Resources- Account Management)