West Texas A&M University™

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY

ACCESS CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
AC-2	**Account Management**	**P1**	**07/02/2017**

I. STATEMENT AND PURPOSE

To prevent unauthorized access to the University's information systems. Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from one state organization to another or from a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization.

Access to West Texas A&M University information resources is commonly controlled by a logon ID associated with an authorized account. Proper administration of these access controls is important to ensure the integrity of University information and the normal business operation of University-managed and administered information resources.

II. 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 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 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 need or benefit to the University exists.

6. 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.

7. All logon IDs that have not been used/accessed within a period of six months shall be disabled. Exceptions can be made where there is an established unit procedure. These actions shall be reviewed and approved by the unit head. Documentation of exceptions shall be maintained by the information resource owner or designee.

8. Passwords associated with logon IDs shall comply with the university system password management standard administrative procedures.

9. Information custodians or other designated staff:

    i. Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to university information resources.

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

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