TARLETON STATE UNIVERSITY
Member of The Texas A&M University System

Information Technology Services
Security Control Standards

NIST Control Family – Access Control

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
AC-2	Account Management	P1	4/15/2020	4/15/2021

I. Statement

Access to Tarleton State 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. Applicability

The intended audience for this control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

III. Risk Statement

To prevent unauthorized access to information systems.

IV. Implementation

A. 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.

B. 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.

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

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

E. Processes are required to disable logon IDs that are associated with individuals who 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.

F. All new logon IDs that have not been accessed within a reasonable period of time (as established by risk management decisions) from the date of creation will 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.

G. Passwords associated with logon IDs shall comply with identification and authentication security controls