Information Technology Services
Security Control Standards

NIST Control Family – Access Control

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
AC-3	Access Enforcement	P1	4/15/2020	4/15/2021

I. Statement

The University enforces approved authorizations for logical access to the system in accordance with applicable policy. Access policies and management ensures enforcement of approved authorization for logical access to information technology resources. 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 security of confidential information and normal business operation of University-managed and administered information.

II. Applicability

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

III. Risk Statement

Misconfigured access controls provide unauthorized access to information held in application systems.

IV. Implementation

As specified in Control AC-2, Account Management, and Control AC-5, Separation of Duties, the procedures for granting, controlling, and monitoring of access to information technology resources are appropriately managed and enforced.