Information Technology Services
Security Control Standards

NIST Control Family – Access Control

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW
AC-17	Remote Access	P1	4/15/2020	4/15/2021

I. Statement

Tarleton State University establishes, documents, and reviews usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. All remote access connections must be authorized prior to allowing such connections.

1. It is the responsibility of Tarleton employees, contractors, vendors, and agents with VPN privileges to Tarleton networks to ensure that their remote access connection is given the same consideration as the user's on-site connection to Tarleton.

2. It is the responsibility of all employees with VPN privileges to ensure that unauthorized users are not allowed access to Tarleton internal networks.

3. At no time should any Tarleton employee provide their login or email password to anyone else, not even family members.

4. When actively connected to Tarleton's network, the VPN connection will force all traffic to and from the computing device (PC laptop, tablet) over the VPN tunnel; all other traffic will be dropped.

5. Split tunneling is not permitted; only one network connection is allowed. If non-work related network access is needed, the employee should first disconnect the VPN

II. Applicability

This Control applies to all Tarleton network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. Risk Statement

Users of Tarleton information systems expose business information to exploitable vulnerabilities when teleworking.

IV. Implementation

Tarleton employees shall take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely (e.g., not leaving laptops and other devices unattended or in public plain view). Employees shall understand their responsibilities for protecting Personally Identifiable Information (PII) data, and the consequences for mishandling PII.