Information Technology Services
Security Control Standards

NIST Control Family – Access Control

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
AC-18	Wireless Access	P1	4/15/2020	4/15/2021

I. Statement

Tarleton establishes usage restrictions, configuration and connection requirements, and implementation guidance for wireless access. Tarleton also authorizes wireless access to the information system prior to allowing such connections.

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

Unauthorized parties gain access to resources by exploiting vulnerabilities in unsecured wireless networks.

IV. Implementation

Requests for wireless service must be architected, engineered, provided, and maintained by Network Services. Vendors and/or external service providers are not authorized to engineer network or wireless services without the explicit approval of network services or the Tarleton IRM. Requests for wireless service within any departmental networks must be approved by Network Services and/or the IRM.

1. Network Services will install and maintain all wireless access points, to ensure they meet minimum security requirements (i.e. changing of SSID).

2. Requests for wireless service for stand-alone networks must also be approved by Network Services.

3. The attachment of unapproved wireless access points, bridges, and/or repeaters is strictly prohibited at Tarleton State University.

4. Wireless access must be password protected and access must be linked to an individual through authentication mechanisms.

5. Network Services will monitor for unauthorized wireless access points. Any such rogue access point detected on the Tarleton State University network shall be disconnected from the network and a security incident will be filed with the information security officer (ISO).

6. Confidential information, mission critical or sensitive personal information shall not be accessed by wireless communication unless the communication is at least encrypted by strong encryption as determined by the information security officer (ISO).

7. Information resource security controls must not be bypassed or disabled.

8. The manufacturer default settings of the Service Set Identifier (SSID) shall be changed upon Initial configuration of any wireless access device.