Information Technology Services
Security Control Standards

NIST Control Family – Security Assessment and Authorization

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
CA-3	System Interconnections	P1	4/15/2020	4/15/2021

I. Statement

Tarleton State University information systems that have connections from the information asset to other information systems outside of the authorization boundary must be authorized and reviewed by the ISO and CIO. Tarleton must monitor information assets connections on an ongoing basis verifying enforcement of security requirements.

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

Security breaches occur due to risks related to external parties not being identified and controlled.

IV. Implementation

All system interconnections with external information resources shall be approved by the chief information security officer and documented. System connection agreements shall be established with all outside information providers/consumers for non-publicly accessible information prior to establishing a system interconnection. Firewall rules shall be implemented to limit access to internal, non-publicly accessible information resources and monitored by the chief information security officer.