West Texas A&M University™

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY
ACCESS CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
AC-17	**Remote Access**	**P1**	**07/02/2017**

I. STATEMENT

WTAMU 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 WTAMU employees, contractors, vendors, and agents with VPN privileges to WTAMU networks to ensure that their remote access connection is given the same consideration as the user's on-site connection to WTAMU.
2. It is the responsibility of all employees with VPN privileges to ensure that unauthorized users are not allowed access to WTAMU internal networks.
3. At no time should any WTAMU employee provide their login or email password to anyone else, not even family members.
4. When actively connected to WTAMU'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 connection.

II. APPLICABILITY

This Control applies to all West Texas A&M network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. IMPLEMENTATION

WTAMU 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.