



**Information Technology Services  
Security Control Standards**

**NIST Control Family – Physical and Environmental Protection**

CONTROL NUMBER	CONTROL NAME	PRIORITY	CREATION DATE	REVIEW DATE	REVISION DATE
PE-1	Physical and Environmental Protection Policies and Procedures	P1	12/13/2019	1/27/2020	2/11/2020

**I. Overview**

The Tarleton State University Information Security Controls Catalog establishes the minimum standards and controls for University information security in accordance with the state's Information Security Standards for Institutions of Higher Education found in Title 1, Chapter 202, Texas Administrative Code (TAC 202).

**II. Purpose**

To develop, document, and disseminate a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and to establish procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and to review and update the associated policy and procedures.

**III. Scope**

The scope of these regulations and procedures are applicable to all information resources owned or operated by Tarleton State University. All users are responsible for adhering to this policy. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

**IV. Risk Statement**

Unauthorized parties have access to facilities due to security flaws in physical layout.



## V. Regulations and Procedures

The State of Texas Department of Information Resources (DIR) has chosen to adopt a select number of Physical and Environmental Protection Controls as established within the NIST SP 800-53 control family guidelines identified by the DIR Security Control Standards Catalog. Tarleton State University shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction.