Information Technology Services
Security Control Standards

NIST Control Family – Audit and Accountability

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
AU-1	Audit and Accountability Policy and Procedures	P1	4/15/2020	4/15/2021

I. Overview

This document establishes the information security audit and accountability regulations and procedures for managing risks from inadequate event logging and transaction monitoring. The information security audit and accountability program helps Tarleton State University implement security best practices related to information security auditing and accountability.

II. Purpose

To implement select information security control standards for the Audit and Accountability (AU) Control family, as identified by the Texas Department of Information Resources (DIR) and the National Institute of Standards and Technology (NIST). The establishment of the Audit and Accountability Control policy and procedures (AU-1) provides a standard for managing risks associated with user account management, access enforcement and monitoring, separation of duties, wireless, and remote access.

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 these regulations and procedures. Information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

IV. Risk Statement

Critical business processes and sensitive data are compromised due to flawed inspection process.

V. Regulations and Procedures

The State of Texas Department of Information Resources (DIR) has chosen to adopt a select number of Audit and Accountability Control (AU) elements as established within the control family guidelines identified by the DIR Security Control Standards Catalog.

Tarleton State University must develop, adopt or adhere to a formal, documented audit and accountability for regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Information resources will be reviewed during the risk assessment process to determine if information systems provide the necessary means whereby authorized personnel can audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.