Information Technology Services
Security Control Standards

NIST Control Family – Audit and Accountability

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULE REVIEW DATE
AU-2	Audit Events	P1	4/15/2020	4/15/2021

I. Statement

All Tarleton State University information resources must be capable of auditing actions of users deemed necessary by the Information Security Officer (ISO).

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 access and activity is undetected due to incomplete log information.

IV. Implementation

A. Consistent with Control *SI-4 Information System Monitoring*, the university shall monitor the use of information systems, maintain security-related system logs, and retain logs in accordance with the university records retention schedule.

B. Information resource custodians shall ensure that information resources have the ability to audit and establish individual accountability for any action on an information resource that can potentially cause access to, generation of, modification of, or affect the release of confidential and controlled information.

C. Audit logs shall be monitored and/or reviewed as risk management decisions warrant. A sufficiently complete history of transactions shall be maintained to permit an audit of the information resources by logging and tracing the activities of individuals through the system Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems, shall be enabled.

D. All suspected and/or confirmed instances of successful intrusions shall be immediately reported to incident management procedures.


TARLETON
STATE UNIVERSITY
Member of The Texas A&M University System