Information Technology Services
Security Control Standards

NIST Control Family – Identification and Authentication

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
IA-5	Authenticator Management	P1	4/15/2020	4/15/2021

I. Statement

Tarleton State University manages information system authenticators by:

A. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
B. Establishing initial authenticator content for authenticators defined by the organization;
C. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
D. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
E. Changing default content of authenticators prior to information system installation;
F. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
G. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
H. Protecting authenticator content from unauthorized disclosure and modification;
I. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
J. Changing authenticators for group/role accounts when membership to those accounts changes.

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 users gain access through user accounts based on a password that was disclosed during communication to the authorized users.

IV. Implementation

The University manages information system authenticators by defining initial authenticator content; establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and changing default authenticators upon information system installation.