BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

SUBJECT: *Information Systems Identification and Authentication*
EFFECTIVE DATE: March 1, 2020; amended October 2022; amended September 19, 2023
BOARD POLICY REFERENCE: CS

PURPOSE
Develop policies and procedures for identifying, authenticating and authorizing access to information systems.

PROCESS
Identification and Authentication Policy and Procedures (IA-01)
The College District establishes policies for verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an information system.
Unique identifiers will be assigned for each individual who has a business or educational need to access College District information resources. A standardized naming convention maintained by Academic Technology will ensure each user's identifier is unique. A method of authenticating the user's identifier will be enabled on each information resource.

Identification and Authentication Policy and Procedures (Organizational Users) (IA-02)
Each user of information resources must be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification must be authenticated before the information resources system may grant that user access.
Unique identifiers will be assigned for each individual who has a business or educational need to access College District information resources. A method of authenticating the user's identifier will be enabled on each information resource.
Shared user accounts are not to be created and distributed without an exception approved by the information system owner and CISO. This does not include local system administrative or root accounts.

Identifier Management (IA-04)
A user's access authorization must be appropriately modified or removed when the user's employment or job responsibilities within the state organization change. User authorization reviews must be conducted according to the related departmental procedures maintained by Academic Technology. The procedure includes the need, scope, frequency and responsibility for the user authorization reviews.

The College District's Human Resources department must notify Academic Technology and/or Administrative Computing of changes in employment status. These status changes will be submitted into the Technology Help Desk system. Workflows will be created to enumerate and track the necessary account changes including but not limited to creating, disabling and modifying authorizations.

The College District's student information system will provide status regarding student accounts to the identity management system to authorize access to information resources and licenses based on current semester enrollments. Authorization will be added, modified and removed based on semester enrollment and course enrollment.

Authenticator Management (IA-05)
The College District 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.

The College District uses passwords as the primary authenticator. A multifactor authentication is used when access to a resource is determined by risk assessment to be of critical nature.

Passwords are confidential information. Passwords should be changed when confidentially is in doubt and when it is a default.

User account passwords should be passphrases of longer length. The passphrase parameters are maintained in a password procedure by Academic Technology.

System account passwords should be randomly generated of longer length. The password parameters are maintained in a password procedure by Academic Technology.

Forgotten passwords must not be reissued. A replacement must be set. The password management system should be used to reset user passwords. Logs of password resets must be maintained for a minimum of 90 days.

Passwords must be encrypted via current encryption standards when in transit and at rest.

Multifactor authentication must be used for access to single sign-on (SSO), VPN and virtual desktop access from off-network along with privileged accounts. Employees should provide their own multifactor device as prescribed by Academic Technology. If they are unable, a physical device can be provided by the College District upon request.

Authenticator Feedback (IA-06)
The authentication system must obfuscate the password entry. Failed authentication feedback does not reveal the failed component.

Cryptographic Module (IA-07)
The authentication system must utilize current cryptographic standards meeting current federal laws, executive orders, regulations, standards and guidance for such authentication.

Identification and Authentication (Non-Organizational Users) (IA-08)
Non-organizational users and processes must be assigned unique identifiers and authentication. Non-organizational users are identified by pre-fix in usernames and categorizing attributes.

Re-Authentication (IA-11)
Require users to re-authenticate when sign-on sessions expire, inactivity time-outs are exceeded or a log-off is initiated.