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 establishes the 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 information resources. A standardized naming convention maintained by Information 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 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 Chief Information Security Officer (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.

The College's Human Resources department must notify Information Technology of changes in employment status. These status changes will be submitted into the Information Technology Help Desk. Established workflows will be created to enumerate and track the necessary account changes including but not limited to creating, disabling and modifying authorizations.

The College'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 manages information system authenticators by:

- defining initial authenticator content;
- establishing administrative procedures for initial authenticator distribution, for lost/compromised, ordamaged authenticators, and for revoking authenticators; and
- changing default authenticators upon information system installation.

The College uses passwords as the primary authenticator.

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

User account passwords should be passphrases of minimum 8 characters in length.

System account passwords should be randomly generated with a minimum 15 characters in length.

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.

Authenticator Feedback (IA-06)

The authentication system must obfuscates the password entry. Failed authentication feedback does not reveal the failed component.

Cryptographic Module (IA-07)

The authentication system must utilizes 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.

- Temple College is responsible for IT regulatory compliance as specified by the Department of Education, the Texas Higher Education Coordinating Board, and the State of Texas Administrative Code (TAC202) for Information Technology. The IT policies include the specific guidance, requirements, and procedures in line with the regulatory and audit requirements.