

1.08.03.00 Digital Identity, Authentication Management, and Access Control (formerly G-051 & G-052)



Policy/Guideline Area

Governance, Organization, and General Policies

Applicable Divisions

TCATs, Community Colleges, System Office, Board Members

Purpose

The purpose of this policy is to establish a minimum expectation with respect to digital identity authentication methods, access controls, and password construction to protect data stored on computer systems throughout the TBR system.

Definitions

- Authentication: A process that allows a device or system to verify the unique identity of a person, device, or other system that is requesting access to a resource.
- Digital identity: Information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. Also referred to as a user account or user profile.
- System account: A special account used for automated processes without user interaction or for device management. These accounts are not assigned to an individual user for login purposes.
- Privileged account: An account with elevated access or privileges to a secure system or resource. This type of account is authorized and trusted to perform security-relevant functions that an ordinary user account is not authorized to perform. Privileged accounts are assigned to individual users. The College System of Tennessee – the system office and affiliated institutions

Policy/Guideline

I. Secure Authentication Methods

- A. Secure methods that uniquely identify the user shall be used for authentication of access to all TBR and institutional networks and systems. Examples of secure authentication methods include passwords, two-factor authentication (2FA), biometrics,

and public/private key pairs.

II. Password (and Passphrase) Construction

- A. To safeguard institutional data access, it's essential to establish and maintain robust password management protocols. All users are obliged to create secure passwords for network and system access in alignment with the given guidelines (except when technological limitations prevent adherence).
- B. Instead of conventional passwords, passphrases may be utilized. Passphrases are exempt from complexity requirements.
- C. Both passwords and or passphrases shall be at least 14 characters long at a minimum.
- D. Passwords should include at least three out of the following four character types:
 - 1. Uppercase letters
 - 2. Lowercase letters
 - 3. Numbers
 - 4. Special characters or symbols (when allowed by the software)

III. Password Management

A. Storage and Visibility

- 1. Passwords must not be stored in a manner which allows unauthorized access.
- 2. Passwords will not be stored in a clear text file.
- 3. Passwords will not be sent via unencrypted e-mail.

B. Changing Passwords

- 1. If 14-character passwords or longer and or passphrases are used, there is no requirement for routine password expiration/rotation. Otherwise, users must change their passwords every 120 days.
- 2. Passwords must be changed within one business day if any of the following events occur:
 - a. Unauthorized password discovery or usage by another person
 - b. System compromise (unauthorized access to a system or account)
 - c. Insecure transmission of a password
 - d. Accidental disclosure of a password to an unauthorized person
 - e. Status changes for personnel with access to privileged and/or system accounts
- 3. Password files or hashes should not be shared with any entity without formal written consent.

C. System Accounts

1. System accounts are not required to expire but must meet the password construction requirements above (where supported by the underlying technologies).
2. Vendor-provided passwords must be changed upon installation using the password construction requirements above (where supported by the underlying technologies).

IV. Multi-Factor Authentication (MFA)

- A. Multi-factor authentication (MFA) is required to be used by all users with public-facing access to critical systems such as information systems, email, or remote access such as virtual private networks (VPN).

V. Access Controls

- A. Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls.
- B. Protection for information assets must be commensurate with the classification level assigned to the information.
- C. Each computer system shall have an automated access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type.
- D. All users of secure systems must be accurately identified; a positive identification must be maintained throughout the login session, and actions must be linked to specific users.
- E. Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

VI. Access Privileges

- A. Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role.
- B. Authorized access shall be based on least privilege, meaning only the minimum privileges required to fulfill the user's role shall be permitted.
- C. Access privileges shall be defined to maintain appropriate segregation of duties to reduce the risk of misuse of information assets.
- D. Any access granted to data must be authorized by the appropriate data trustee.
- E. Access privileges shall be controlled based on the following criteria as appropriate:

1. Identity (user ID)
2. Role or function
3. Physical or logical locations
4. Time of day/week/month
5. Transaction-based access
6. Access modes such as read, write, execute, delete, create, and/or search

F. Privileged access (e.g., administrative accounts, root accounts) must be granted based strictly on role requirements.

G. The number of personnel with special privileges should be carefully limited.

VII. Access Account Management

A. User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection.

B. The following requirements apply to network logons as well as individual application and system logons and should be implemented where technically and procedurally feasible:

1. Account creation requests must specify access either explicitly or request a role that has been mapped to the required access.
2. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.
3. Accounts must be locked out according to individual campus requirements after an institution-defined number of consecutive invalid logon attempts.
4. When a user account is locked out, it should remain locked out for a minimum of five minutes or until authorized personnel unlock the account.
5. User interfaces must be locked according to individual campus requirements after an institution-defined length of system/session idle time.
 - a. This requirement applies to workstation and laptop sessions as well as application sessions where feasible.
 - b. The office of information technology shall implement measures to enforce this requirement and to require the user to re-authenticate to reestablish the session.
6. Systems housing or using restricted information must be configured in such a way that access to the restricted information is denied unless specific access is granted.
7. Access to restricted information is never to be allowed by default.

8. Information Technology personnel revoke access upon notification that access is no longer required in accordance with the following procedures:
 - a. Access privileges of terminated or transferred users must be revoked or changed as soon as notification of termination or transfer occurs.
 - b. In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneously with departure.
 - c. Access for users who are on leaves of absence or extended disability must be suspended until the user returns.
 - d. Access to Banner Admin Pages is consistently denied to adjunct faculty members. The procedure for managing access for adjunct faculty accounts is established at the local institution level, incorporating defined dates of employment according to contract status and integrating input from entities responsible for adjunct contract oversight. Each institution, guided by its academic calendar and directives from contract control authorities for adjunct faculty, will implement this specified procedure on a schedule set by the respective campus. The scope of this process is to be defined by each individual campus, ensuring that adjunct faculty have restricted access beyond their designated course timelines to fulfill job requirements, which may be extended upon a justified request detailing specific access needs.
9. User IDs will be disabled after a period of inactivity that is determined appropriate by the current business process and the individual campus.
10. All third-party access (contractors, business partners, consultants, vendors) must be authorized and monitored using processes determined by the individual campuses.
11. Appropriate logging will be implemented commensurate with the sensitivity/criticality of the data and resources.
12. Logging of attempted access must include failed logons.
13. Where practical, successful logons to systems with restricted information shall be logged.
14. Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity.
15. Logs shall be maintained for at least ninety days.
16. A periodic audit of secured systems to confirm that access privileges are

appropriate must be conducted. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.

17. Applications requiring an account not tied to a single user shall employ service-based accounts. Users oversee these accounts and maintain their passwords.
18. Applications requiring these accounts shall be monitored and audited by individual campus documented procedures dictated by the application for which they are provisioned.
19. Service-based accounts due to their application-centric use are not subject to standard user account management rules.

VIII. Compliance and Enforcement

- A. The policy applies to all users of information resources, including students, faculty, staff, temporary workers, vendors, and any other authorized users.
- B. Persons in violation of this policy are subject to a range of sanctions determined and enforced by the individual institutions, including the loss of computer network access privileges, disciplinary action, dismissal from the institution, and legal action.
- C. Some violations may constitute criminal offenses per Tennessee and other local and federal laws. The institution will carry out its responsibility to report such violations to the appropriate authorities.
- D. Documented exceptions to this policy may be granted by the information security officer for the institution based on limitations to risk and use.

Sources

References

[NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions](#)

Authority

T.C.A. § 49-8-203

History

NEW guidelines G-051 & G-052 approved at Presidents Meeting, August 19, 2014, effective September 26, 20-14; revisions, including merger of G-051 and G-052 into the policy, approved at Special Called Meeting May 14, 2019; revisions approved at Board Meeting September 20, 2024.

