MONTGOMERY COLLEGE

Office of Information Technology

IT Standard

INFORMATION TECHNOLOGY RESOURCE AUTHENTICATION

Standard:	IT08001
Original Effective Date:	11/30/2009
Last Revised:	07/01/2021
Last Reviewed:	07/01/2021
Next Scheduled Review Date:	07/01/2022
Version No.:	4.2
Administrative Owner:	Information Security and Privacy Director

The purpose of this document is to provide the minimum standards by which authenticated access to Montgomery College ("College") information technology resources is established, applied, and managed. The College requires individuals that access its technology resources and application systems to authenticate themselves as authorized network and application users. The College expects its community members to comply with all direction regarding the creation, usage, and safeguarding of electronic identifiers and passwords and be vigilant in protecting College technological and information assets.

SCOPE

This Standard applies to all employees, contractors, students, vendors and other agents who have access to Montgomery College technology resources and application systems.

DEFINITIONS

Term	Definition
Authentication	The process by which the identity of a subject is verified when requesting access to systems and/or network resources.
Individual Account	A user account that identifies a specific/unique person or process.
Privileged Account	A user account with additional or special access to a system or application such as the ability to make configuration changes, perform maintenance, modify security, or perform other critical system or application tasks.
Generic Account	A user account that does not identify a specific/unique person or process such as guest or admin.

STANDARD

A. General

1. Authentication must occur prior to accessing any College system or application, which has not been designed for public viewing.
2. Existing authentication systems (e.g. Active Directory, LDAP) must be used to provide authentication services when possible.
3. UserIDs must be unique and created in a consistent format across systems and applications.
4. A user must authenticate to systems and applications using their unique UserID.
5. Default UserIDs initially shipped with purchased software must be disabled upon system installation or the default passwords initially shipped with the software must be updated.
6. Clear-text passwords must not be 'hard-coded' into scripts or other files.

7. Passwords must be masked on computer screens when being entered.
8. An account password must be changed when any individual knowledgeable of its value no longer has responsibility to access the account.
9. Account UserIDs must be disabled when an individual no longer requires access to College technology resources or application systems.
10. An account password must be changed if there is any suspicion that the password has been compromised.
11. IT Staff will never ask users for their passwords.
12. The IT Security Group (ITSG) will audit compliance to this standard.

B. Passwords

1. Passwords must be treated as confidential information and protected. Passwords must not be posted in plain sight or where they can be easily disclosed. They must be stored and/or transmitted in an encrypted format.
2. Passwords must be created to accommodate the specific rules and constraints of the system or application in which they will be used.
3. At a minimum, passwords must:
   a. be at least eight characters in length.
   b. not contain personal information about the account holder or information specific to an automated process.
   c. contain valid password character attributes such as:
      1) Upper-case letters
      2) Lower-case letters
      3) Numbers
      4) Special characters such as ! @ # $ % ^ & +
4. Passwords must not be reused.
5. Forgotten passwords must not be retrieved. Passwords must be reset after verification of identity.

C. Individual Accounts

1. Passwords associated with Individual Accounts must not be shared.
2. Individual Account passwords must include at least 2 of the valid password attributes identified in Section B.3.c of this document.
3. The initial passwords generated for Individual Accounts must be set to expire and require the user to change the password upon first login.
4. Individual Account passwords must be changed within 180 days.

D. Privileged Accounts

1. Use of generic Privileged Accounts such as Administrator and Root are to be used by OIT employees and contractors only. Use of these accounts must be restricted.
2. The system administrator, group manager or supervisor directly responsible for an IT system or application must be able to identify all users with access to generic Privileged Accounts.
3. The sharing of Privileged Account passwords must be restricted and controlled. When it is necessary to share a password associated with a privileged level account in order to manage an IT system or application, a password security process must be established by the responsible system administrator and communicated to all relevant team members.
4. Privileged Accounts must be vaulted in a Privileged Account Management system identified by OIT (e.g. Password Manager Pro).
5. Privileged account password must be at least 15 characters long.

EXCEPTIONS

This standard is applicable as of its Effective Date. Exceptions to this standard will be considered on a case-by-case basis in accordance with the IT Exception Request Form.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, or vendor found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
November 30. 2009	Original roll-out of this IT Resource Authentication document.	Patrick Feehan, Information Security and Privacy Director/ITPA
May 9. 2018	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson
July 1, 2021	Minor clean-up edits during review cycle. (E.g. – change CyberArk to Password Manager Pro)	Nell Feldman, IT Security Manager