Office of Information Technology

IT Standard
SYSTEM AND APPLICATION ACCESS MANAGEMENT

Standard:	IT11001
Original Effective Date:	05/23/2012
Last Revised:	04/04/2022
Last Reviewed:	04/04/2022
Next Scheduled Review Date:	04/04/2023
Version No.:	1.3
Administrative Owner:	Director of Information Security Services

PURPOSE

It is the policy of Montgomery College ("College") to protect and promote secured access to its information technology resources. The purpose of this document is to provide the minimum standard by which access to College systems and applications resident on its networks is granted and managed. Access to College resources is restricted to the minimum level of access required to perform a College approved function.

SCOPE

This standard applies to Montgomery College personnel who are responsible for governing or managing access to College systems and applications.

DEFINITIONS

Term	Definition
Access Management	The process of granting authorized users the right to use a resource while preventing access to non-authorized users.
Confidential Information	Defined by College Policy 66002, Confidential Data Management and Security as: Confidential Information includes but is not limited to the following: the personnel record of any past or present employee; any record containing PII; credit or debit card data; student information which has not been identified as directory information (see Board Policy #41003 Student Cumulative Records); records or material that have otherwise been identified as confidential, subject to trademark or a copyright protection, or for which there is a contractual limitation on disclosure; records of the Office of General Counsel, or any records of which exposure unnecessarily invades personal privacy or impairs individual rights.
Administrator Account	An account with privileged or elevated access permissions to a system or application that provides the user the necessary permissions to make configuration changes, perform maintenance, modify security, or perform other critical system or application tasks.
Standard Account	An account without privilege or elevated access permissions to a system.

User Account	General reference to a Standard or Administrator account.

STANDARD

A. General

1. All individuals working on behalf of the College with permissions to grant and maintain access privileges to College systems and applications have the responsibility to comply with existing College Policies and IT Standards and protect College academic and administrative information and computer technology resources.
2. By default, all administrative and academic user accounts are assigned least access privileges.
3. College units must have documented processes for granting, monitoring, revoking, and otherwise managing access to College IT systems or applications.
4. Non-employees of the College that require access to College systems and applications must have their access sponsored by a College administrator or their designee.
5. OIT will audit compliance to this standard.

B. Access Management

1. Granting authorized users the right to use a resource must represent the minimum level of access required to perform the job function associated with the user.
2. College supervisors are responsible for monitoring and managing their direct report employees and contractors account access to College IT systems or applications. The managers and supervisors are responsible for ensuring that the above referenced minimum level of access is maintained during the course of the employee's job assignment.
3. College supervisors are responsible for ensuring that all access is removed upon termination of duties caused by but not limited to a job change, placement on administrative leave, or termination of employment.
4. Access to confidential information should be assigned to the data element level.

C. User Accounts

1. User Accounts must be removed when they are no longer required or have met their expiration date. This includes but is not limited to an employee placed on administrative leave, employee termination, or employee job responsibility change.
2. User Accounts must be disabled after a period of inactivity equal to 90 days unless directed otherwise by an OIT standard or College policy.

D. Application and System Controls

1. User accounts must lock after a maximum of five(5) invalid authentication attempts. The account should remain locked for a period of 15 minutes or until unlocked by the responsible system administrator.
2. User Account sessions must timeout after a period of inactivity equal to at most 65 minutes.
3. Administrative account access such as "root" or "system "administrator" must be restricted in order to protect the confidentiality, integrity, and availability of College systems and applications and all associated data.

E. Temporary Administrative Access

1. In some cases, the College may grant temporary administrative access to an employee to a College-owned device based on business justification.

2. College applications that require elevated privileges beyond the standard user permissions are managed by the IT Security Group (ITSG).
3. Administrative access will be assigned to, and may only be used by, one specific user who will be designated as the owner of the account. Per the Acceptable Use Policy, the user is solely responsible for all activities performed as an Administrator, and any consequences of those actions.
4. Administrative access should only be used for the duration of time necessary to perform functions requiring elevated permissions. At all other times, standard user accounts must be used.

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 Standard 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

- Montgomery College Policy 66001, Acceptable Use of Technology
- Montgomery College Policy 66002, Confidential Data Management and Security
- IT Process- IT11001A _Administrative Access

WEB SITE ADDRESS FOR THIS STANDARD

https://info.montgomerycollege.edu/offices/information-technology/it-security/it_standards.html

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
May 23, 2012	Original roll-out of this System and Application Access Management document.	Patrick Feehan, Information Security and Privacy Director/ITPA
February 21, 2018	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson
April, 2022	Revised.(Added temporary administrative access and a point of clarification added to General (2). Minor grammatical changes. Website address added).	Nell Feldman, Interim Director of Information Security Services/CISO/IT Policy Administrator

Nell Feldman Digitally signed by Nell Feldman
Date: 2022.04.07 13:03:48 -04'00'