Office of Information Technology

IT Standard
REMOTE ACCESS

Standard: IT11002
Original Effective Date: 08/12/2008
Last Revised: 07/15/2021

Last Reviewed: 07/15/2021
Next Scheduled Review Date: 07/01/2022
Version No.: 3.2
Administrative Owner: Director of Information Security Services

PURPOSE

It is the policy of the Board of Trustees ("BOT") of Montgomery College ("College") "to offer teleworking at an off-site location as an effective way to meet the needs of the College, its employees, and the community". The BOT has further mandated that the College Network be protected, as directed by the Chief Information Officer ("CIO") and the Office of Information Technology ("OIT"). The responsibility for ensuring Remote Access for teleworkers as well as employees, contractors, vendors and agents belongs to OIT.

The purpose of this Standard is to define and describe the requirements for Remote Access. Compliance to this Standard and Processes minimizes the (1) potential exposure of College Network to unauthorized use and, (2) the risk of confidential data loss, and (3) damage to the College's public image or its technological infrastructure.

SCOPE

This Standard applies to all Remote Access connections to the Montgomery College Network, including those used to read or send email, access intranet web resources, use the College's VPN gateways, or access via other technologies approved by IT. All Departments of the College are affected by this Standard. All members of the College community interested in teleworking or Remote Access should read this Standard.

DEFINITIONS

Term	Definition
Telework	The practice of working at home or another work site instead of traveling to College offices.
Remote Work	The practice of working from home or another work site that is outside the College's geographic area.
College Network	All technology equipment, infrastructure, software resources and any related technology resources that are administered, allocated and managed by and for the College, are considered to belong to the College Network, whether in a networked environment or stand alone, including equipment owned by the College used in an off-site location.
Personal Firewall	An application which controls network traffic to and from a computer, permitting or denying communications based on a security standard. Personal firewalls are typically used on personal computers.
Two-factor authentication	An added second level of security during the login process to help prevent anyone other than the user from accessing systems storing sensitive data. This is accomplished using two layers of security to verify the user's identity when authenticating (logging) into a system: 1. Username (your MyMC ID) with your password

	2. Use a physical device such as a cell phone, tablet or landline phone to confirm your identity
Remote Access	Proper, secure and authorized access to Montgomery College's Network through a non-Montgomery College controlled network, device, or medium.
Agent	Anyone with permission and acting on behalf of the College other than an employee, contractor, or vendor.
Contractor	An individual representative of a business external to Montgomery College who has been assigned to an IT work group for a set period of time to supplement its work staff. The individual may reside either at an IT facility or at an offsite facility not within the College boundaries. The individual reports directly to a College IT supervisor or manager in addition to their own business management.
Vendor	An external business entity contracted by Montgomery College for a set period of time for the purpose of providing a service or delivering a product.
Internal Network	The section of the College Network that is not directly accessible to the public and for which there are special access privilege requirements.

STANDARD

Remote Access privileges will only be granted to employees and third parties if authorized in a Process that includes approval of a College administrator and, in the case of a third party, additional approvals as deemed necessary. Additionally, Remote Access will be limited to applications necessary and for the time necessary for the specific needs of the Remote Access user. A Process will include how a Remote Access privilege is revoked upon violation of this Standard, violation of applicable College Policies (including but not limited to the Acceptable Use of Information Technology Policy) or IT Standards or Processes, or when Remote Access is no longer necessary. Any application for Remote Access will be reasonably reviewed and verified as necessary before the access is allowed.

Authorized users of the College Network may be permitted to remotely connect to that network for College related business only through secure, authenticated and carefully managed access methods. Each Remote Access connection must comply with the following requirements:

A. College employees, contractors, vendors and agents with Remote Access privileges to the College's Network have the responsibility to comply with existing College Policies and IT Standards and protect College academic and administrative information when accessing the College Network.

B. Additional information regarding the College's Remote Access connection options, including applying for remote access, is available on the Montgomery College OIT website under Forms, Account/Access Requests, Remote Access (VPN) Request.

C. Secure Remote Access is allowed to the College’s Microsoft Office 365 tenant and MyMC (web portal) via a SSL enabled internet connection. All other Remote Access will be controlled via the College’s VPN gateways.

D. Remote Access users must protect their College Network and email logins and passwords at all times and never share this information.

E. Remote Access users must not use non-College email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct College business, thereby ensuring that official business is never confused with personal business.

F. All hosts that are connected to the College Internal Networks via Remote Access technologies must use the most up-to-date anti-virus technology.

G. All hosts that are connected to College Internal Networks via Remote Access technologies must use personal firewall technology.

H. All organizations or individuals connecting via the College's VPN gateways must use the College's two-factor authentication (2FA) solution.

I. Organizations or individuals who wish to implement non-standard Remote Access solutions to the College Network must consult with and obtain prior approval from the IT Security Manager.

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 or as approved in writing by the Director of Information Security Services.

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

- Acceptable Use Policy and the accompanying Procedure/Guidelines Statement
- College Telework Policy for Administrative, Associate, and Support Staff
- IT11002A: Virtual Private Network Process

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
August 12, 2008	Original roll-out of this Remote Access document.	Patrick Feehan, Information Security and Privacy Director/ITPA
August 2015	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA

February 21, 2018	Revised. (Version 3.0)	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates. (Version 3.1)	Nell Feldman / Keith Wilson
July 15, 2021	Minor grammatical clean-ups, updated location of VPN request form, reflect new title of Director of Information Security Services.	Nell Feldman, Interim Director of Information Security Services.