MONTGOMERY COLLEGE

Office of Information Technology

IT Process
VIRTUAL PRIVATE NETWORK (VPN)

Process:	IT11002A
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

The purpose of this Process is to define and describe the rules for remote VPN connections to the Montgomery College network. Compliance to this Process minimizes (1) the potential exposure of College Network to unauthorized access, (2) risk of intellectual property or confidential data loss and (3) damage to the College's public image or its technological infrastructure.

SCOPE

This Process applies to all Montgomery College employees, contractors, vendors and agents that utilize a VPN gateway to access the Montgomery College network from non-trusted networks. This Process applies to all implementations of VPN at Montgomery College.

DEFINITIONS

Term	Definition
Virtual Private Network (VPN)	An encrypted network that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
Personal firewall	An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. 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
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.
Agent	Anyone with permission and acting on behalf of the College other than an employee, contractor, or vendor.

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.
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.

PROCESS

A. GENERAL

1. Only Administrator approved Montgomery College employees and authorized third parties (contractors, vendors, agents, etc.) may utilize the VPN.
2. Montgomery College employees (including both staff and faculty), contractors, vendors and agents with VPN access privileges to Montgomery College's network have the responsibility to abide by the requirements of this document. They must comply with existing College Policies and IT Standards and protect College academic and administrative information when accessing the College’s technology resources.
3. The IT Security Group (ITSG) will conduct periodic reviews of users with VPN access to verify it is still required, and terminate access for any users who no longer have a need for remote access.
4. ITSG will terminate access for any VPN users who no longer have a relationship with the College through resignation, termination or discontinuation of services.

B. REQUIREMENTS

Each user who accesses the College Network through a VPN connection must comply with the following requirements.

1. It is the responsibility of users with VPN privileges to ensure that unauthorized users are not allowed access to Montgomery College Internal Networks. Application for VPN access shall be reasonably reviewed and verified, as necessary, by a representative of ITSG. Both time limits and access limits may be implemented as appropriate for any VPN access.
2. Authorization for **employee, contractor, vendor and agent** VPN access privileges is obtained through the submittal of the Remote Access (VPN) Request form located on the Montgomery College OIT_website under Forms, Account/Access Requests, Remote Access (VPN) Request. Once submitted, the form triggers a Service Desk workflow that requests both supervisor and administrator approval. Once approved, ITSG will set up VPN access and provide appropriate documentation and instruction to the requesting user. Upon termination of the employee, VPN access will be terminated.
3. VPN use is to be controlled using a strong password consistent with applicable College Policies and IT Standards.
4. Contractor, vendor and agent VPN users are required to have a MyMC user name and password. To obtain a MyMC account, the user’s supervisor is required to fill out the Personal Data Form located on the HRSTM webpage https://cms.montgomerycollege.edu/uploadedFiles/EDU/Departments_-_Administrative/Human_Resources/HRSR/Records/Personal%20Data%20Form%20Updated%2004272015.pdf
5. VPN users are required to enroll in the College’s 2-factor authentication (2FA) solution, and access will only be granted after authenticating with their MyMC user name, password and the 2nd factor.
6. VPN gateways will be set up and managed by Montgomery College network operational groups.
7. All hosts that are connected to Montgomery College internal networks via remote access technologies must use the most up-to-date anti-virus technology.
8. All hosts that are connected to Montgomery College internal networks via remote access technologies must use personal firewall technology and have their system up-to-date with the current patches.

9. VPN users will be automatically disconnected from Montgomery College’s network after twelve hours. The user must then logon again to reconnect to the network. Pings or other artificial network processes must not to be used to keep the connection open.
10. VPN provides secure access into the Montgomery College network. VPN does not, by itself, provide Internet connectivity. Users are responsible for providing their own Internet access to be able to use Montgomery College VPN service.
11. To use VPN technology with personal computing equipment, users must understand that their machines are an extension of the College Network, and as such must be configured to comply with IT Standards and are subject to the same rules and regulations that apply to Montgomery College-owned equipment.

EXCEPTIONS

Exceptions to this process will be considered on a case-by-case basis in accordance with the IT Exception Request Process.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies and IT Standards and Processes to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, Contractor, Vendor or other Agent found to have violated any part of this Process and related Standard as well as other College Policies, Standards or Processes while having a remote connection will have their remote access immediately revoked and may be subject to disciplinary action.

The College reserves the right to remove or suspend VPN privileges or any other remote access options if the computers are not kept current with anti-virus, firewall software, and appropriate operating system patches. IT will review VPN access on a yearly basis.

RELATED DOCUMENTS

- Montgomery College Policy 66001, Acceptable Use of Technology
- Montgomery College Policy 32500, College Telework Policy
- IT11002: Remote Access IT Standard

WEB SITE ADDRESS FOR THIS PROCESS

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
August 12, 2008	Original roll-out of this Vulnerability Scanning 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, update of VPN definition, extended VPN disconnect time from 20 minutes to 12 hours, updated location of VPN request form, reflect new title of Director of Information Security Services.	Nell Feldman, Interim Director of Information Security Services.