Security Guidance for Working Remotely

Article Number: 8175 | Rating: Unrated | Last Updated: Fri, Mar 13, 2020 at 9:54 AM

MONTGOMERY COUNTY COMMUNITY COLLEGE

2020

Security Guidance for Working Remotely

Whether it's a typical part of your job or as an alternative if access to campus is temporarily restricted, the ability to work remotely (also known as telecommuting or teleworking) can help keep the College's operations running. Though potentially a great benefit to your department's operations, it's essential that all remote work be performed in a securing computing environment.

Preferred method

The most secure method for working remotely is to plan ahead and issue MC3/college-owned computers for staff members to use remotely.

Work can be performed directly on the MC3-issued computer, or the computer can be used to connect remotely to the staff member's virtual desktop (https://mc3.edu/citrix) residing on campus.

The setup requires:

- **MC3-issued and professionally-maintained laptop**

A laptop issued to an employee in advance of working remotely, or a laptop available as needed in an emergency situation, is the best option or working remotely. These laptops should meet all required security standards for handling sensitive data and should be maintained by the IT department following best practices for system management.

- **College VPN**

Use of the MC3 provided VPN software gives staff members access to defined systems for working remotely, allowing connections to sensitive campus system to be restricted and secured.

- **A broadband Internet connection**

The MC3 VPN is a full tunnel; all network traffic will traverse the VPN.

Acceptable method

If use of MC3-owned equipment for employees to facilitate remote work is not an option, a staff member's personal computer may be used to connect remotely to a virtual desktop

residing on campus (https://mc3.edu/citrix).

For reasons of both security and policy, College work must not be performed directly on a staff member's non-MC3-owned equipment. Such equipment should be used only to connect to a remote computer (https://mc3.edu/citrix), on which all work is performed.

This setup requires:

- **Personal (non-MC3-owned) computer**

An employee's personal computer can be used as a mechanism to connect to a remote virtual desktop residing on campus. Personal computers should be maintained in a secure fashion (with regards to passwords, malware and virus protection, etc.) and should be to the extent possible, up-to-date with the latest operating system and security updates.

- **Microsoft Azure multi-factor authentication (MFA)**

The use of Microsoft Azure MFA is required to establish a secure connection. A staff member connecting remotely will need to enroll in Microsoft Azure MFA (https://mc3.edu/mfa) via the Microsoft Authenticator mobile app, security token, text message, or phone call. **This must be configured prior to connecting from off-campus!**

NOTE: Staff members should ensure that, if an office telephone is currently used to authentication via Azure MFA, an additional factor (such as a personal mobile phone or a home phone) is added as an authentication method.

- **A broadband Internet connection**

Collaborating effectively while working remotely

Working remote may pose challenges for staff accustomed to collaborating in-person on campus. Several services have been approved to facilitate workplace communications and team collaboration, and may be quite helpful when normal means of collaborating are unavailable.

Specifically, approved tools useful for remote work include:

- Microsoft OneDrive for document sharing and collaboration (https://kb.mc3.edu/article/onedrive-office-365-overview-and-usage-6075.html)
- Microsoft Teams for text messaging, video conferencing and screen sharing (https://kb.mc3.edu/article/microsoft-teams-your-online-teamwork-hub-8167.html)
- Blackboard Collaborate for video conferencing, screen sharing and remote instruction
- Office365 for email and calendaring (https://kb.mc3.edu/article/office-365-overview-of-microsoft-office-365-suite-6073.html)

Before storing or sharing sensitive data, please consult the College Data and Storage System Quick Reference

(https://kb.mc3.edu/article/college-data-and-storage-system-quick-reference-847.html)

Telephone usage while working remotely

Access to voicemail from off-campus is supported (https://kb.mc3.edu/article/accessing-staff-faculty-voicemail-from-off-campus-47.html)

Access to voicemail from an MC3-issued computer is supported via the website https://vmail.mc3.edu

Access to voicemail from a non-MC3-owned equipment is supported via the virtual desktop environment https://mc3.edu/citrix

A computer can also be used to receive and place telephone calls to/from campus phone numbers. By using a VoIP "soft client"—computer software that mimics the capabilities of a standard desk phone—a remote staff member can place calls from, or answer incoming calls to, his or her campus phone number directly from his or her computer. VoIP soft client functionality requires the use of the MC3 VPN and may require pre-authorization by the IT Department.

Questions

Please contact us at helpdesk@mc3.edu with any questions about securely performing remote work.

Posted - Tue, Mar 10, 2020 at 2:52 PM. This article has been viewed 744 times.
Online URL: https://kb.mc3.edu/article/security-guidance-for-working-remotely-8175.html