Are you ready to work remotely?

Using your CUIMC-provided laptop is the best option for working remotely. However, if you don’t have a CUIMC laptop and need to use your personal computer, please follow the necessary steps to prepare.

Don’t forget to do a test-run to make sure your equipment works as expected!

Remember, even though you’re working remotely, you’re not alone. If you need help, you can contact your local IT Help desk or visit https://it.cuimc.columbia.edu.

Considerations to walk through at your remote location:

1. Think about the files and applications you’ll need to access from home.
   - It will be extremely important to save all work-related data and files to either the cloud or a security-certified shared drive (not the laptop/desktop/endpoint).
   - Zoom video conferencing can be accessed from any web browser.
   - Office 365 applications such as email, calendar, OneDrive and SharePoint can also be accessed online here:
   - Most other major CUIMC applications are available at https://it.cuimc.columbia.edu
   - Talk to your manager if you think you’ll need access to department shared drives (like your O: Drive or P: Drive). The CUIMC IT Help Desk staff can help you learn about available options.
     - Critical documents can be moved over to Microsoft Teams to ensure they are accessible while working remotely.

2. Please ensure that your personal computer is updated and secure.

If you do not have a CUIMC-provided laptop, you will need to take extra steps to make sure your information stays secure. We have provided a list of steps that are Mandatory for all CUIMC users to follow in order to work on computers in remote locations (including at home):

<table>
<thead>
<tr>
<th>Automatic Updates for Microsoft Windows Computers:</th>
<th>Click on this link to view instructions on keeping your Windows computer up to date.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Updates for Apple Mac Computers:</td>
<td>Click on this link to view instructions on keeping your Mac up to date.</td>
</tr>
<tr>
<td>Prevent Unauthorized Access on Microsoft Windows Computers:</td>
<td>Use these steps to prevent unauthorized access on your Windows computer:</td>
</tr>
<tr>
<td>1. Open the Start Menu</td>
<td></td>
</tr>
<tr>
<td>2. Select Control Panel</td>
<td></td>
</tr>
<tr>
<td>3. Choose Windows Defender Firewall from the menu shown below and turn it on.</td>
<td></td>
</tr>
</tbody>
</table>
Prevent Unauthorized Access on Mac Computers: Use these steps to prevent unauthorized access on your Mac:

1. Choose System Preferences from the Apple menu.
2. Click Security or Security & Privacy.
3. Click the Firewall tab.
4. Unlock the pane by clicking the lock in the lower-left corner and enter the administrator username and password.
5. Click "Turn on Firewall" or "Start" to enable the firewall.

Click Advanced to customize the firewall configuration.

Enabling Encryption on Microsoft Windows Computers: Home versions of Windows do not offer hard disk encryption. If you have a professional version of Windows, encryption is provided with BitLocker. You can configure it by following these steps:

1. Search for “BitLocker Drive Encryption” in the search box on the bottom left side of the screen.
2. The box shown below will pop up. Select “turn on BitLocker”.
Enabling Encryption on Mac Computers: FileVault provides encryption for MacOS. To enable it, navigate to Apple menu, then “System Preferences”, then “Security & Privacy”. Click the FileVault tab and then Turn on FileVault.

Locking Your Screen on Microsoft Windows Computers:
You can lock your computer screen by simultaneously pressing Windows Key and the L key on your keyboard or by simultaneously pressing Ctrl, Alt, and Delete then choosing Lock when the list of options pops up.

Locking Your Screen on Mac Computers Go to the Apple menu and choose “Lock Screen” or simultaneously press Command, Control, and Q.

3. Gather everything else you’ll need to be productive
   - Does your computer have a built-in microphone and speaker?
   - Do you need a headset for your phone?
   - Don’t forget any important work files or other equipment, like power adapters, that you’ll need to bring home from the office
   - Set up a device (such as a mobile phone) that you have access to remotely for two-step verification. You won’t be able to verify your identity if you’re not there.

4. Bookmark https://it.cuimc.columbia.edu

You can visit our IT website from outside CUIMC and get access to technical information and applications you need. Below is a snapshot of some of the available resources.