SCHOOL OF PUBLIC HEALTH
UIC Information Services

Remote Work Preparation Checklist

March 12, 2020

Background

This checklist is designed to help faculty and staff in the UIC School of Public Health prepare to work from home. It is not meant to imply that the ability to work from home has been authorized for you.

Essential things to consider

- ☐ **Home Office using SPH Equipment –** You will need a high-speed network connection and device setup at your home / home office.
    1. Bring your laptop home each night in the event you may need it and the University asks staff to stay home.
        a. If you don't have a device of working remotely in an emergency, Contact your department head to let them know at this time, ahead of the need.
        b. A limited supply of loaner devices is available for use. Contact SPHhelp for more information.
- ☐ **Home Office using personal computing equipment** – Please refer to Appendix A
- ☐ **Documents - Box -** Save any relevant work papers (but not research data sets) to U of I Box at http://uofi.box.com so you can easily work with them wherever you may be.
- ☐ **Remote Access** – Test your ability to connect to your SPH office computer before needing to work remotely.
    1. If you do not have VPN access, request it by sending an email to sphhelp@uic.edu In your request, include a specific business justification for why you need VPN access.
    2. Ensure VPN is set up on the device you will be using. Almost all UIC systems require VPN for remote access (Banner, TEM, FrontEnd, Eddie, etc.)
        a. Download the VPN software from the WebStore at https://webstore.illinois.edu/shop/product.aspx?zpid=3652
        b. Install DUO 2-Factor Authentication (2FA) on your mobile device. Instructions are located at https://answers.uillinois.edu/page.php?id=67790
            a. NOTE: You can only setup Duo while **on campus**.
            b. NOTE: VPN access set up through SPH will only work for SPH resources and the University Library. If you need access to other college's VPN networks, contact the college directly.
            c. Set up VPN using the appropriate instructions
                i. MacOS – http://apps.sph.uic.edu/webdocs/AnyConnect_MAC.pdf
                ii. Windows - http://apps.sph.uic.edu/webdocs/AnyConnect_windows.docx
    3. If you are still unable to connect after performing the above, contact sphhelp@uic.edu or 312-355-2618.
- ☐ **Voicemail -** You can remotely change your phone's voicemail message and are able to set up your phone to send you emails once you receive a voicemail

- There are two systems
  - VoIP Voicemail (most people are using this) - https://voicemail.uic.edu/
  - Unity Voicemail System - http://unityw1.voip.uic.edu/ciscopca

☐ **Remote Email –** Remote access to e-mail is web-based. Go to https://outlook.uic.edu

☐ **Host virtual meetings** -

1. Use WebEx to host a meeting – https://uichicago.webex.com
   a. If you plan on hosting a meeting, it is best if you download and install the client from the WebEx web page.
      i. People who are simply attending a meeting do not need a client, just send them the URL and call-in information WebEx provides you for the meeting you have scheduled
   b. Host a test meeting in advance to familiarize yourself and your colleagues with the technology.
   c. A headset or landline phone is best for audio. Mobile phones frequently breakup and are not suitable for hosting a conference call. Additionally, a wired, high speed network connection is best although a high-speed wireless connection should work in most cases.
2. Microsoft Teams can be used for virtual collaboration - https://accc.uic.edu/services/communication-collaboration/virtual-collaboration-spaces/microsoft-teams/

SPHIT Support

Office Hours: 8:00 AM - 5:00 PM, M-F

- Helpdesk Tickets may be opened via the following methods:
  - E-Mail – sphhelp@uic.edu
  - Phone - (312)996-8736

SPH IT will maintain continuity of IT support during contingency scenarios as much as possible, within the HR guidelines of the University and College.

In addition, please consult the following/below resources from the University related to working remotely:

- ACCC Tech Resources for Working Remotely: https://accc.uic.edu/news-stories/tech-resources-for-working-remotely/
- ACCC Tech Resources for Teaching and Learning Online: https://accc.uic.edu/news-stories/tech-resources-for-teaching-learning-online/

Appendix A – Home office with non-SPH provided computers

While using VPN from personal computers (that is, non-university purchased computers) may be convenient, it is not suitable in some cases. For example, if you work with sensitive or high-risk data, such as research data with PHI, admissions data, HR or personnel data, you should not use a personal computer for this work as the University IT Security Policy requires that access to this type of data only be performed on university-provided computers that have been appropriately secured.

If you are a faculty member in SPH, for normal teaching purposes using a personal computer is fine as long as it complies with the University security policies. However, if you are doing research with PHI or other personally identifiable information, that work should be done on a university-supplied machine.

For staff and others in administrative roles, personal computers should not be used for any work involving sensitive data. This includes all data for which there are legal requirements to prevent disclosure or financial penalties for disclosure, such as credit card information, as well as all information covered by federal and state legislation, such as the federal Health Insurance Portability and Accountability Act (HIPAA) or the Illinois Personal Information Protection Act (IL PIPA).

In addition, if you use a personal computer you must ensure the functionality you require is available. The SPH Help desk is not able to provide assistance for equipment that is not owned by UIC.

Even if you are not working with sensitive or high-risk data, you still must ensure that your computer complies with the requirements of the UIC IT Security Policy if you are using it for university business. The policy requires the following set of conditions be met:

1) Endpoint protection software, such as Windows Defender or Symantec Anti-virus, must be installed and active
2) Automatic updates for the operating system and other software must be enabled
3) The machine must “auto-lock” after a brief period of inactivity (no more than 20 minutes) to ensure that the device cannot be used by others if left unattended
4) All accounts on the personal computer must have passwords which meet the requirements defined at https://password.uic.edu
5) Accounts on the computer must not be shared among users
6) UIC passwords must not be “remembered” in any software including web browsers
7) Passwords should not be stored on the device unless encrypted with a password manager such as LastPass