CASet Tech Operation and Remote Support

The following information outlines CASet support related to distance learning, working remotely and support in response to COVID-19 events.

- All CASet resources are focused on prioritizing workorders that are related to academic continuity to ensure CAS faculty are prepared for remote instruction.

- Be sure to forward and update your UB voicemail appropriately in order to receive calls and to respond to any phone inquiries. http://www.buffalo.edu/ubit/service-guides/phones/managing-your-voip-telephone-service/forward-calls.html

- All technology purchases must be reviewed by CASet before they are made. This will occur through a response to a submitted workorder. The College of Arts and Sciences will either obtain the product for your department or provide approval to move forward with a department purchase. In the case of a department purchase it will be transferred via IDI to the Dean's Office in April as long as there is documented purchase approval from CASet. At this time, all emergency technology costs are planned to be funded by the Dean's Office.

- Users requesting support from CASet must submit a workorder. If you have an emergency issue (for example, you are about to teach online using Webex and are having a problem) then please reach out to us via phone at **716-645-9199**. Please, only use this number for urgent matters related to remote instruction.

- CASet does not have loaner laptops or other equipment to deploy for uses beyond remote instruction. Staff approved to work remotely should use their own equipment to perform their duties.

- CASet staff will be providing support remotely to users when needed. This will require the user to be present in front of their computer since their permission is needed before the remote connection can be established. It may also involve a phone call to provide us with the connection information we may need.

- If you are taking home a University owned device, please reach out to us before taking it home to ensure that you have the necessary software and permissions on the system. In some rare instances, we may not be able to connect to you remotely unless we make some changes on your system. We need to make these changes to your system before it leaves campus.

- CASet will have some loaner PC's, MacBook Airs and iPads available for use. The first priority will be to those faculty/instructors that do not have a laptop available to them or a machine at home that they cannot use. Loaners to staff will only be considered if there are remaining systems after instructors have made their requests.

- If you are provided with a CASet loaner PC or Mac, before leaving campus, be sure to connect the computer to the wired or wireless network and logon to the computer at least once.

- If users wish to connect remotely to their office computers, please submit a work order at https://www.caset.buffalo.edu and we will assist with that. Those users that opt for this option will need to make sure their office computer remains powered on. This will require the use of UB's DUO Two-Factor authentication and in this instance, the DUO FOB/hardware key will not work with it.

- If you are using your own device at home, there are several things that everyone should do to secure their personally owned home computer in preparation for connecting to UB resources from home. These are simple and necessary steps to ensure the security of both your computer and the University's data.

The first step in securing your home machine is to make sure that automatic operating system updates are enabled. Without this, any other security measures you take will be largely irrelevant.

Follow these Steps:

Windows 10:
- Settings -> Update & Security -> Windows Update
- Under "Advanced Options", select "Choose how updates are installed", then select "Automatically"

Windows 7:
- Please be advised that Microsoft is no longer issuing security updates for Windows 7. If you are still using Windows 7, you should give serious thought to upgrading to Windows 10. Regardless, if you are using Windows 7, please enable automatic updates to make sure that you have all updates that have been issued previously.
- Control Panel -> System & Security -> Windows Update
- Under "Important updates", select "Install updates automatically (recommended)"

macOS:
- Under System Preferences -> Software Update, check the box next to "Automatically keep my Mac up to date."

The next step is to make sure that you have up to date antivirus software installed. Your home computer may have come with an antivirus package. Some common antivirus packages that you may see on personal machines are McAfee, Norton, Kaspersky, BitDefender, etc. If you have one of these installed and it is receiving regular virus definition updates, this is fine. If you have one of the above, but it is a trial version or is otherwise no longer receiving updates, you should install Symantec Endpoint Protection, available free of charge from UB.

Windows:
- Download and run the unmanaged SEP installer from the UBIT website:
  - 64-bit (default):
https://download.acsu.buffalo.edu/index.php?sw=licensed/Symantec_Endpoint_Protection_14.2.2_Win64-bit_Client_EN.exe
  - 32-bit (Use this *only* if you are certain that you're running a 32-bit version of Windows):
https://download.acsu.buffalo.edu/index.php?sw=licensed/Symantec_Endpoint_Protection_14.2.2_Win32-bit_Client_EN.exe

macOS:
>   • Download and run the unmanaged SEP installer from the UBIT website:
>>   • 64-bit only:

https://download.acsu.buffalo.edu/index.php?sw=licensed/Symantec_Endpoint_Protection_14.2.2_Mac_Client_EN.zip

Please note, all links provided above are links to the latest version of the software available at the time this document was written. If the links do not work, or if you want to view the latest versions of all software available to UB faculty and staff, please go to https://www.buffalo.edu/ubit/service-guides/software.html.

Many UB resources will only accept connections from on-campus computers by default. In order to access them from off campus, you will need to install a VPN client. The long-standing official VPN client for UB, is the Cisco AnyConnect client. Download, install, and configuration instructions for all operating systems are available here:
https://www.buffalo.edu/ubit/service-guides/connecting/vpn/computer.html

It is also likely that the University will begin using a new VPN client in order to deal with the increase in remote access traffic. Instructions for installing and using this client will be forthcoming.

We understand that these are uncharted waters for everyone. We appreciate your patience and understanding.

Martin Camacho
Assistant Dean for Technology
College of Arts and Sciences