Do you have the necessary tools to work remotely?

To successfully accomplish your tasks and duties remotely, do you have all the tools available to you? Below is a general checklist of tools you may want to ensure you have access to prior to a telecommuting arrangement:

- Email—Do you have access remotely to read and respond to emails throughout the day. Will you be accessing emails via a remote desktop connection, via your phone or through HawkMail?
- Virtual Private Network (VPN)—You should ensure your laptop is equipped with and through the University's VPN. Without this access, you will not be able to remote to your desktop and access your online files. See page below to set up your VPN.
- Job-specific databases—Banner, Raisers Edge, and Compass are just a few. Do you know how to access them remotely? Are your passwords to log in to various systems you utilize secured?
- Skype, Webex, Zoom, Teams—Which platform will you use to keep in communication with your team? What will be the expectation for being "on video"?
- Keep your information and the University's information secure. See below for tips from ITS on securing data.
- Do you know who to contact for assistance with technology issues? ITS HelpDesk (helpdesk@hartford.edu or 860.768.4357).

Connect to campus with the Virtual Private Network

Connecting to the University of Hartford's network from home increases the risk of data exposure or password compromise because you must use networks that are not controlled by the University. To minimize these risks, you should use the campus Virtual Private Network (VPN) when working with sensitive University data. This will ensure that everything you do is encrypted as it goes over the network. VPN protects your data from electronic eavesdropping and may be required to connect to some department and central resources from off campus. To find out how to install and use, see the VPN Install Guide Available.

Secure your home wireless network

Home wireless networks are easy to set up and extremely convenient to use. However, an insecure wireless environment poses several risks that need to be addressed:

- Anyone near your home can use your internet connection.
- Anyone near your home may be able to access your computer.
- Anything sent over the wireless connection could be hacked or stolen.

The manuals that came with your wireless router should provide detailed information on how to secure your home wireless network. If you no longer have the manual, use the brand name and model type to search for an electronic copy online.

Keep your computer secure

If you are working on a computer that is not University owned, make sure that your operating system and applications are updated regularly. In addition, activate your computer's firewall protection and antivirus software. If you're working on University business on a computer at home, regardless of whether the computer is owned by you or the University, you **must** take measures to secure your computer and mobile devices.

Secure Your personally owned device

If you cannot use a University-owned device when working at home, however, please follow the steps outlined below to make sure you are minimizing risk to the University while working remotely.

Use a separate login account

If other members of your household use the same computer, create a separate login account for your University work and data, with a strong password that only you know. Using a separate login ensures other users on your computer cannot view or access your documents.

Encrypt all confidential data

If you have confidential data on a computer that is located at home, or that comes home with you, that data must be encrypted. Check with IT support staff to find out what encryption solutions are used in your department.