Best Practices for Secure Telecommuting

Use Your UAlbany Account

- Always use your UAlbany computing account to conduct University business, even if you have a personal account for the same application. Your University account authenticates you as a member of the campus community, providing full access to campus IT resources.
- **UAlbany Zoom requirements:** Beginning August 15, 2020, all faculty and students will be required to use their UAlbany Zoom account to join any classes using the Zoom platform. This new security measure assures that only those with a UAlbany Zoom account can join a class without waiting to be admitted by the professor.

Keep Your Computer Secure

- University-owned machines: If you are using a University-owned device from off-campus, make sure it is receiving Windows updates.
- Personally-owned machines: If you are conducting University business on a personal device, follow these instructions to make sure your Windows or Mac operating system has the most current updates and is protected with antivirus software.
- Keep University information secure if you’re accessing campus resources from a computer shared with others in your household. Take care to protect confidential information and systems, log out of all applications, and close all browser windows when you’re done working.
- All equipment used for University business must comply with the policy on Connecting Devices to the University Network and Standards for Connecting Devices to the University Network.

Keep Your Files Secure

- Sensitive and confidential data always requires special care. Such information should always be stored on your assigned network drive or, when appropriate, in UAlbany-approved cloud services (i.e., OneDrive for Business, Microsoft Teams). Never store sensitive or confidential data on mobile devices or a third party, personally-maintained cloud services (i.e., Dropbox, Google, etc.).
- ITS provides numerous options for storing your files. The best place to store information depends on the sensitivity of the data and who needs access.
- Always follow the University’s Category 1 Storage Standards to ensure you are storing data appropriately.

Keep Your Connection Secure

- Connecting to the campus network remotely increases the risk of compromise or exposure, as that connection relies on network providers outside the University. These risks are minimized when you connect using GlobalProtect VPN (Virtual Private Network). This encrypts all traffic coming to the campus network, even when connecting from a public or unsecured WiFi connection.
- Use GlobalProtect VPN to access systems containing sensitive or confidential data from off-campus locations.
- ITS recommends securing your home wireless network to prevent others from using your Internet connection or accessing your data. Search the Internet using the make and model of your wireless router if you need instructions.

Go Phish!

- Times of uncertainty present cybercriminals with new opportunities. Always exercise caution before clicking on links or opening unexpected attachments.
- Fake messages have become increasingly sophisticated. Don’t be fooled into compromising institutional or personal information.
- Report suspicious messages easily using Phish Alert. With the simple push of a button, the message is forwarded to the ITS Information Security team for investigation and permanently deleted from your mailbox.

Need more help? Contact the ITS Service Desk.