When working from home it is important to remember to maintain safe cyber security practices for protecting University data and resources. Below are important guidelines to follow while working from home.

What to do before you begin working from home:

- Ensure that you have access to your files. Utilize OneDrive, departmental file shares, etc.
- Leave your office computer turned on and logged out in case you need to access it remotely. If you believe you may need to connect to your office computer, it is important that you test the ability to connect now so that you know it works when you need it.
- If you need to change your password, use the online password tool.
- Contact your campus Support Center for additional support.

Working from home using a University-owned device:

- Connect to the university network using VPN (this is not necessary if only connecting to publicly available web sites).
- Run a full virus scan on your computer once a week to detect any problems.
- Report any suspicious activity on your computer to **security@uh.edu**.
- Avoid giving others physical access to university equipment.
- Level 1 data handling and protection MUST comply with SAM 07.A.08.
- Logout before you walk away from your computer.

If using a personally owned device:

- Ensure you have anti-virus/anti-malware software installed and running on your computer. If you are using Windows 10, free anti-virus is built in. Avast Free Mac Security is an option for Mac users and has received good reviews.
- Run a full virus scan on your computer once a week to detect any problems.
- Report any suspicious activity on your computer to **security@uh.edu**.
- Do not store Level 1 data on your personal device. Level 1 data handling and protection MUST comply with SAM 07.A.08.
- If you are using University Enterprise systems such as PeopleSoft, do not download data onto your personal device. Enterprise system data needs to remain in the enterprise system.
- Logout of University systems after completing your work. Do not remain logged in to university systems on your personal device.
- If you perform any work or create any work product that is considered a university record, it is your responsibility to move the 'university record' off of your personal device and store it on a university- owned device or system as soon as possible.