Security Information for Working from Home

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).

• 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.

http://www.uhsystem.edu/compliance-ethics/_docs/sam/07/7a8.pdf

• Logout before you walk away from your computer.

If using a personally owned device make sure you are running the latest Windows OS, which is Windows 10 on your home computer. Not Windows 7 or XP:

• Ensure you have anti-virus/anti-malware software installed and running on your computer. Windows 10 has a free built-in anti-virus so no need to purchase one. For Macs we recommend installing the latest McAfee anti-virus software.

• Run a full virus scan on your computer once a week to detect any problems.

• Report any suspicious activity on your computer to afts@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. http://www.uhsystem.edu/compliance-ethics/_docs/sam/07/7a8.pdf

• 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 your personal device and store it on a university- owned device, OneDrive, or departmental share drive as soon as possible.