CSUSM Safe Computing Practices

***Secure Home Network* -** IITS will not provide direct configuration assistance of any home network equipment but will perform a basic configuration review with the employee. It is the employee's responsibility to verify and properly configure/secure their wireless network to include:

- **Changing the default administration username and password and setting a secure password** of 10 to 15 characters. The passphrase should not be a dictionary word. The default log in credentials are found quite easily with a quick online search, and therefore are extremely insecure.
- **Turn off Remote Administration**, and to the greatest extent possible, features and functions that make the device accessible to external parties and threat actors.
- **Set a unique SSID** and turn off broadcasting (unless required by the environment).
- **Utilize network encryption** of WPA2 or WPA3 or a direct/wired connection to the router.
- Validate that the router is set to **receive automatic updates from the vendor**

General IT security alertness and prevention helps to protect the University's data. Personal computers are prohibited for processing of Level 1 data unless the personal computer is being used to connect to an approved campus system or service. Employees working from home are to follow these safe computing practices.

- **Username & Password/Passphrases & Multi Factor Authentication (MFA)** – The employee will comply with all CSU/CSUSM password standards and use of MFA on any device or system accessing university data or system.
- **Use of VPN and Encryption** - Every time you log in to a website, make sure that the connection is encrypted. The URL address should start with https instead of http. Where appropriate, utilize the university's security VPN (GlobalProtect), Citrix, or LogMeIn services to access sensitive university systems via a Virtual Private Networks (VPN).
- **Keep devices secure** – Even at home, employees are to lock their screen with a password to safeguard the data on your computer. Additionally, don't allow family members to use your work computer and treat your work computer and sensitive data as if you were sitting in a physical office location
- **Keep Work Data on Work Computers** - The employee should only keep university data on officially supported system and avoid downloading or synching files or emails to a personal device.
- **Proper Storage of Sensitive Information** - Delete sensitive information whenever you can, even from university owned computers. Keep it off of your workstation, laptop computer, and other electronic devices if at all possible. University data is only to be stored on CSUSM owned systems, computer equipment, or officially designated services such as Office 365/SharePoint/OneDrive/Teams.
- **Keep all personal/university information safe** - Reduce your risk of identity theft and never share your personal information or that of anyone in the CSUSM community via email, no matter how official the email looks. Official business that requires personal information should not happen via unsecured email and never use FTP or other services that aren't encrypted.
- **Keep all data confidential** – Be aware of your surroundings and who might be listening to conversations. If you are having a conversation about a sensitive topic, make sure that the room is clear or that others around you cannot hear what you are discussing. Also, when working with sensitive data make sure that no one can see and read the information on your screen.
- **Avoid surfing websites that you don't already know** - Browsers and links in email are the predominate source of introducing malware or vulnerabilities to your computer. It is strongly recommended to stick with the websites you trust when using university computer equipment.
- **Only Download files legally** – Do not download programs, music, or other media to your university owned computer without consulting IITS. Along with the possibility of significant legal penalties, downloading files from peer-to-peer networks can be harmful to your machine. These downloaded files are sometimes riddled with viruses and spyware.