Remote Work Guide for Faculty and Staff
Data Protection Guideline

When working remotely, you may access protected university data, which requires appropriate security protection. This guideline provides direction for securing protected university data while working remotely.

Securely Store Protected Data

Fresno State has three data classification levels consisting of Level 1 (confidential), Level 2 (restricted) and Level 3 (unrestricted) data. The Protected Data Storage Guidelines illustrate what data can be stored and shared using Fresno State's enterprise storage options. These storage options include Google Drive, BOX, Fresno State's Network File Shares and OneDrive. Use one of these approved storage and collaboration options to ensure the security of university data. Do not send confidential data by email. Only keep files and data you need.

Personal cloud storage accounts, personal computers and personal storage devices are not acceptable for storing protected university data (Level 1 or Level 2). You can remotely access campus computers by first connecting to the campus Virtual Private Network.

Secure Paper Files

When there is a legitimate university need to transfer protected data from office to home and it has been approved by your manager, keep it out of sight and under lock and key. If you don't have a file cabinet at home, use a locked room. Dispose of sensitive data securely. Shred it. Don't just throw it in the trash or recycling bin. Paperwork you no longer need can be valuable to identity thieves if it includes personal information about customers, employees or students.

Secure Your Account and Identity

Add extra security to your Fresno State userID with two-factor authentication (2-Step Verification). Two-factor authentication provides a higher level of security for the Fresno State resources and data you access. University faculty and staff are required to use 2-Step Verification. Enroll in 2-Step Verification.

Secure Your Computer and Devices

Keep track of and secure any device that contains protected university data. If using your own personal computer is your only option, take the following additional precautions:

- Update all your devices with the latest operating systems, web browsers and security software.
- Update and configure antivirus protection to safeguard against malicious attacks
- Enable the devices firewall, where applicable
- Encrypt your device, when possible, using whole disk encryption such as
    - Apple MacOS FileVault
    - Microsoft Windows BitLocker
- Do not save your Fresno State userID or password on the computer
- Create a separate account and strong password for each individual using the computer

Secure Your Home WiFi Network

Secure your home network to protect your privacy. Follow these basic steps to secure your home WiFi network:

- Secure your WiFi router by changing the default password assigned by the manufacturer
- Change the name of your WiFi network from the default name assigned by the manufacturer
- Encrypt WiFi traffic. Select WiFi Protected Access II (WPA2) or WiFi Protected Access (WPA)
- Disable remote administration

Beware of Phishing, Scams and Fraud

Be vigilant when opening emails or attachments. Phishing is the most common form of security incidents. Cyber criminals ask you to click on links or download files. Don't click. Be cautious, trust your instincts, click wisely:

- Go directly to a reputable website to access the content
- Click only links that you expect
- Open only files you expect to receive
- Open emails only from people you trust
- If in doubt forward the email to reportphishing@csufresno.edu