Remote-Ready Checklist

Whether you're using your University-managed or personal device, here's how to connect securely

Equipment Check

- Does your computer/laptop have a built-in microphone and speaker?
- Need a web cam or headset?

We may have a loaner for you! csus.edu/laptopcheckout

The Essentials

Connect to campus resources with Global Protect VPN especially if using public Wi-Fi

Make sure you can authenticate off-campus via DUO. How To's at csus.edu/duo

Get up to speed at csus.edu/zoom

Bookmark directory.csus.edu to look up colleagues

Bookmark portal.office.com to access Outlook, Teams, OneDrive, and more. How to's at csus.edu/microsoft365

Find other available software/tools at csus.edu/irt/software

Device Security

Read IT Security Guidance for Remote Access

Never share passwords, and protect them with a strong password manager like the free LastPass app

Avoid using external storage devices like USB drives. If you must, ensure the device and data is encrypted

Level 1 data may only be accessed using University-managed devices, and may only be stored on SacFiles Secure

Remote work = no backups. Use Microsoft OneDrive or SacFiles to store your data

Call Forwarding

- Forward desk phone to an alternate number
- Forward your voicemail to email
- How to remotely access/change voicemail settings

If you have your office phone set up for Duo Verification, learn how to add an alternate device