



eMEMO

CITRUS COMMUNITY COLLEGE DISTRICT 1000 W. Foothill Blvd., Glendora, CA 91741-1899

Technology and Computer Services (TeCS) Update

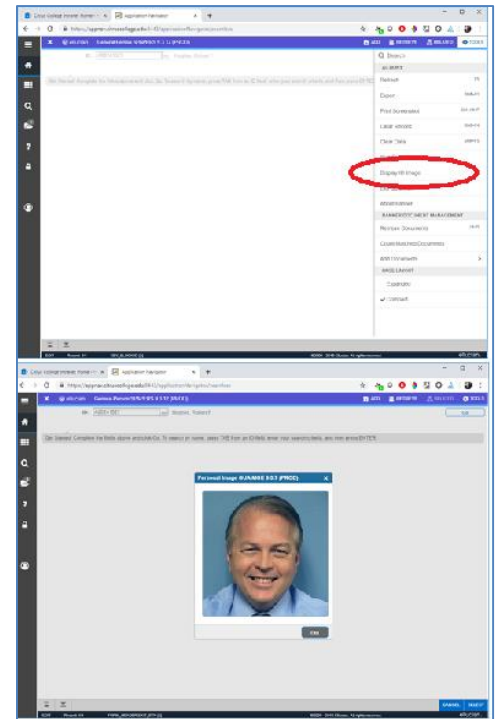
July 2019

Photo ID images in WingSpan

Photos from our photo ID system have now been integrated into WingSpan. If you are logged in to any screen in WingSpan that is linked to a 'person' record (in other words, you have to enter a student or employee ID number in the 'Key Block'), simply click on the 'Tools' icon, then click 'Display ID Image'. You will then be able to view the photo ID picture that is connected to the record on your screen.

Staff in student services areas can use this feature to assist in confirming student identities before releasing sensitive or FERPA-related information. Our next project is to connect images to class rosters so faculty can more easily identify students registered for their classes. We plan to provide this enhancement later this year.

Mike Maliglig, Mark Chan and Leigh Buchwald were instrumental in delivering this new feature.



Video Wall in the Campus Center

You are probably familiar with massive video displays on billboards, stadiums and arenas. Resolution on video display technology has improved dramatically in recent years, and prices have dropped significantly. Consumers can now purchase a 50-inch 4K ultra high definition flat screen television for under \$300.

While massive video displays are still quite expensive, more affordable systems can be created by merging multiple smaller displays into a video wall.

TeCS has configured a portable video wall comprised of four large monitors that can replace a projector and screen for use in the Campus Center.



Print Stations for Student Printing

TeCS partnered with Dr. Gina Hogan and faculty from the Hayden Memorial Library to install six print stations on campus for student use. Students can now print wirelessly from a laptop, mobile device, a USB drive, from an e-mail or from documents uploaded to the web simply by logging in to a print station with their network account.

Print stations are located in the campus center, the first and second floor of the library, in the math building lobby and in the lobby of student services. Print stations are constantly monitored by the vendor to ensure they are functional and stocked with paper and toner.

Costs for printing range from 12 cents for a single-sided black and white document to 99 cents for a double-sided color document, and all major credit cards are accepted for payment.

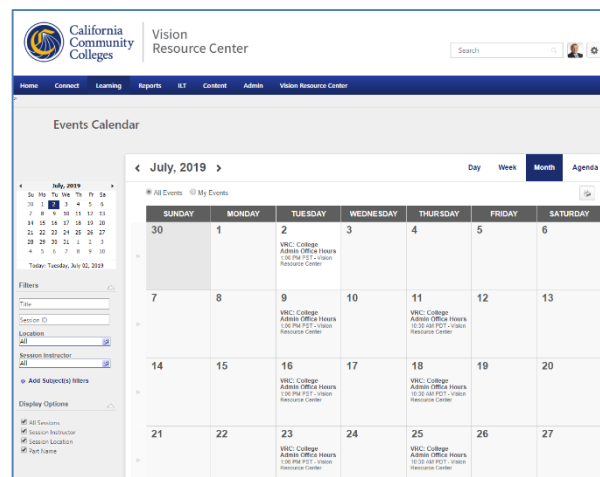
These devices have been shown to increase the ease of printing for students, protect privacy and reduce waste at colleges and universities across the country. In our local area, they are in use at APU, Cal State Fullerton, USC, UCLA, UC Riverside, UC Irvine and Antelope Valley College. For more information, see <https://libguides.citruscollege.edu/print>.



Training Calendar for Faculty and Staff Development

TeCS is pleased to announce the availability of the Citrus College Training Calendar. This system, also known as Cornerstone On Demand or the Vision Resource Center, is provided at no cost thanks to the CCC Chancellor's Office.

With this tool, employees can easily sign up for training classes being offered on campus. You will be able to see past training classes that you've attended, access a transcript of your professional development, and sign up for recorded, self-paced training courses in topics like Microsoft Office applications, leadership and customer service through SkillSoft and Lynda.com.



Another important feature is the ability for faculty and staff to create and participate in Facebook-like learning communities where you can chat and share documents with other CCC professionals around specific topics.

Training classes on the Training Calendar will be held on the following dates and times in July:

- Monday, July 22 at 3 pm
- Thursday, July 25 at 3 pm
- Thursday, July 25 at 9 am
- Friday, July 26 at 1:30 pm

Sign up by logging in to the Training Calendar at <https://my.citruscollege.edu/task/all/training-calendar---vision-resource-center>. Click on your desired date/time and then click 'Request' to be added to the class roster.

Security Matters – Keeping Tabs on Mobile Devices

With an increasing amount of sensitive data being stored on personal devices, the value and mobility of smartphones, tablets, and laptops make them appealing and easy targets. These simple tips will help you be prepared in case your mobile device is stolen or misplaced.

- **Encrypt sensitive information.** Add a layer of protection to your files by using the built-in encryption tools included on your computer's operating system.
- **Secure those devices and backup data!** Make sure that you can remotely lock or wipe each mobile device. That also means backing up data on each device in case you need to use the remote wipe function. Backups are advantageous on multiple levels. Not only will you be able to restore the information, but you'll be able to identify and report exactly what information is at risk.
- **Never leave your devices unattended in a public place or office.** If you must leave your device in your car, place it in the trunk, out of sight, before you get to your destination, and be aware that the summer heat of a parked car could damage your device.
- **Password-protect your devices.** Give yourself more time to protect your data and remotely wipe your device if it is lost or stolen by enabling passwords, PINs, fingerprint scans, or other forms of authentication. Do not choose options that allow your computer to remember your passwords.
- **Put that shredder to work!** Make sure to shred documents with any personal, medical, financial, or other sensitive data before throwing them away.
- **Be smart about recycling or disposing of old computers and mobile devices.** Properly destroy your computer's hard drive. Use the factory reset option on your mobile devices and erase or remove SIM and SD cards.
- **Verify app permissions.** Don't forget to review an app's specifications and privacy permissions before installing it!
- **Be cautious of public Wi-Fi hot spots.** Avoid financial or other sensitive transactions while connected to public Wi-Fi hot spots.
- **Keep software up to date.** If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.

What can you do if your laptop or mobile device is lost or stolen? Report the loss or theft to the appropriate authorities. These parties may include representatives from law-enforcement agencies, as well as hotel or conference staff. If your device contained sensitive institutional or student information, immediately report the loss or theft to Technology and Computer Services so that we can respond quickly to the incident.

Monthly content for Security Matters is courtesy of the [EDUCAUSE Cybersecurity Program](#).