Don’t Lose Wi-Fi Access on Campus

In addition to an easier one-time log-in to UF’s Wi-Fi system for users on the main campus, security enhancements were also made, including checking that devices connecting to the Wi-Fi network have up-to-date anti-virus software and firewall protection.

Starting July 16, any laptop or wireless device trying to connect to UF’s Wi-Fi without the minimum security requirements will be redirected to a site providing documentation and links to anti-virus software. Wireless access will not be available until minimum security requirements are met.

Not sure if your laptop or mobile device is up-to-date? It’s easy to check. Visit: getonline.ufl.edu.

Faculty and staff using UF-owned computers to connect to the university’s Wi-Fi should first contact their department IT group to update that machine.

Why is UF doing this?

With new and more destructive malware attacks reported daily every effort must be made to protect UF’s networks that carry research data, administrative information and student records. The anti-virus check also serves as a reminder to all users that their files and personal information is worth protecting, too!

WCBA Personnel and Students

If Warrington faculty and staff have any questions please contact your IT Team Member or put in a CBAHelp request for assistance. One of your team members will assist you.

Students will need to contact the TAC for support with their devices.

For help call (352-392-HELP), visit (132 HUB), or email the UF Computing Help Desk.

CBAHELP System Change - One Service is No Longer Available

The CBAHELP system can no longer accept the “reply” e-mails used in the past to send additional comments to your technician or automatically re-open your CBAHELP.

The system still supports all the other functions you’ve become accustomed to. You just can’t respond to the CBAHelp Request any longer.

If you need to send additional information to your technician, please submit a new CBAHELP or contact your technician direct.

We are actively researching a replacement for the CBAHELP system.

In addition to the CBAHELP system, you may contact the Technology Assistance Center for emergencies (273-0248) and they will contact your department technician for you.
Secure Flash Drives and Protecting Laptop Hard Drives is a UF Requirement

University of Florida policy requires all portable drives and mobile devices containing university data be encrypted to protect UF data.

Last November an unencrypted USB flash drive was stolen from a University of Miami faculty member. What was on that that flash drive? Personal information on more than 1,200 of his patients. USB ‘flash’ drives can hold a lot of data, but are easy to lose or have stolen.

If we notice unsecure flash drives in your office or classrooms, we will follow-up with an email providing you with the information needed to purchase new secured flash drives.

DMBTC has started installing laptop hard drive encryption software on all new and repaired laptops. We are now requesting that all WCCA-owned laptops be brought in so we can install the encryption software. We will also upgrade the OS and install patches as needed. If we determine that the laptop is too old for OS upgrade we will work with you to find a solution.

Please work with your department IT Support Team to schedule a time for us to install this upgrade. Please allow 3 days to complete the upgrade.

Additional Security Measures for UF Faculty and Staff

UF Policy and Your Responsibility

Policy

All mobile computing and storage devices that access the University of Florida Intranet and/or store University of Florida restricted data must be compliant with University of Florida Information Security Policies and Standards.

Restricted data stored on mobile computing and storage devices must be encrypted.

Any and all mobile computing devices used within the University of Florida information and computing environments must meet all applicable UF encryption standards. Mobile computing devices purchased with University of Florida funds, including, but not limited to contracts, grants, and gifts, must also be recorded in the unit’s information assets inventory.

University of Florida information security policies applicable to desktop or workstation computers apply to mobile computing devices.

Responsibilities

The University of Florida Information Security and Compliance Office will establish standards to govern the secure use of all mobile computing and storage devices at the University of Florida.

The University of Florida Office of the Vice President and Chief Information Officer will provide guidance to assist units in complying with these requirements.

All University of Florida deans, directors and department chairs, in conjunction with their IT support teams, are responsible for migrating all existing uses of mobile computing and storage devices within their areas of responsibility to devices and services that are compliant with university policies and standards.

All members of the University of Florida constituency who are using personally-owned mobile computing and storage devices that access the University of Florida Intranet and/or store University of Florida Restricted data are required to bring their personal device into compliance with the University of Florida Information Security Standard for Mobile Computing and Storage Devices.

All members of the University of Florida constituency will report the loss or theft of a mobile computing or storage device to their departmental Information Security Manager (ISM) immediately upon detection of the loss. The UF Privacy Office must be immediately notified of theft or loss of any portable computing device or media that contains restricted data.

Please help us protect UF data.