Computer Lab Security

Our computer labs employ a combination of physical and software-based methods to ensure the safety and security of our students, faculty, staff, equipment, and computer network.

Restriction of Computer Lab Access

All Information Technology computer labs are secured by card-swipe or proximity locks, as well as scheduled electronic locks, to ensure that only authorized persons are able to enter and use the labs during regularly scheduled hours.

Physical Security

All Information Technology computer labs are secured through card-swipe or proximity locks, as well as scheduled electronic locks, to ensure that only authorized persons are able to enter and use the labs during regularly scheduled hours. In addition, IT computer labs are monitored either in person by a lab technician, remotely through security cameras, or a combination of the two. When possible, equipment is placed to limit access to physical ports on the CPU as well, especially for teaching equipment located in podiums.

Software Based Security and Prevention of Installation of Malicious Software

In addition to the standard anti-virus and anti-spyware clients installed on each campus computer, all Information Technology Computer lab computers are further protected either through group policy, security software, or a combination of the two to prevent malicious software from being installed and executed. As a further security measure, all campus computers require a unique, authorized login for authentication before granting network access.

Reporting Theft, Damage or Suspicious Behavior

First and foremost, be safe. If you notice something in an Information Technology computer lab that you deem suspicious or unsafe, move to a safe area outside of the computer lab. Then, contact either the Help Desk at 410-677-5454 or Public Safety at 410-543-6222 (#787 for Verizon users).

Related articles

Content by label

There is no content with the specified labels