Our computer labs employ a combination of physical and software-based method 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-swatch 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 computers lab computers and assets are locked down through cabling or other means to enhance physical security. 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).