# Wells College
# Information Technology Policies
# Physical Security Policy

*Approved May 2018*

## Policy Statement

Wells College is committed to following State and Federal Regulations and IT Best Practices to implement security controls for mitigating risks and protecting the confidentiality, integrity, and availability of the college's information assets. Proper physical security controls, ongoing monitoring, and auditing will help to ensure that the College's business continuity meet legal compliance.

## Purpose

This policy defines the requirements for protecting Wells College information and technology resources from physical and environmental threats to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference of Wells College operations. Physical security includes measures to protect resources against unlawful and unauthorized intrusion. Environmental threats include protecting resources from damage resulting from fire, flood or other physical threats.

## Scope

This policy applies to all staff and faculty, as it addresses threats to critical IT resources that result from unauthorized access to facilities of Wells College containing critical IT resources or sensitive information, data centers, network closets, and similar areas that are used to house such resources. Staff and faculty work areas that contain computer equipment that can connect to sensitive systems of the college's computer network must also have security controls in place. Staff and Faculty who travel and use portable devices that connect to the Wells College computer systems must also protect those assets.

## Expectations

### 1) Staff and Faculty Offices

Staff and faculty computers log onto a separate virtual local area network (VLAN), which unlike lab and classroom computers available to students can access servers that may contain sensitive and protected data. Therefore the following security measures shall be followed.

Staff and faculty should arrange their offices in such a way, where displays should not be viewable from guests should there be sensitive confidential or protected information displayed on the screen. If the office arrangement will not allow for screen privacy, to limit viewing of the display and if sensitive information is routinely accessed, screen filters or others means of making the display hard to read should be implemented.

The computers should be put in the “locked mode” when an office is unoccupied for short periods of time. If the office is to be unoccupied for an extended period, the computer should be locked or logged off of and the office door locked.

Only the assigned staff or faculty member(s) should use the computer in their office space.

IT shall conduct periodic training sessions and have information posted regarding physical security and protection of IT resources across campus and while traveling.

IT staff offices and storage areas should be keyed separately from the common master key strategy used across campus for other offices, classrooms, etc..

### 2) Data Center and Switch Closets

IT facilities containing servers, switches and other core IT infrastructure are only to be accessible by IT Staff who need access as part of their job function at the college. No other unauthorized access shall be permitted. Security and Facilities personnel should notify the Director of IT if they need to or have had to access these facilities for safety or security purposes.

Data Centers, rooms containing core network switches and servers shall be locked at all times and have a secure key that is not part of the Master Key system implemented across campus. Only authorized IT personnel, the Director of Security and the Director of Buildings and Grounds should also have access for emergency purposes only. Data Centers should not be shared spaces with other purposes and should not be used as storage rooms. Whenever possible, existing IT facilities should look to include electronic access systems, such as card swipes and door alarms and security cameras to the facilities. All new facilities should have these security controls included in the construction.

A log book is located in all Data Center facilities and all staff entering the room(s), must log the date and time and reason for accessing the facility. These log books shall regularly be audited to make sure staff, faculty or vendors needing to access secure spaces are logging in their visits.

Data Closets, rooms or closets containing network switches, but no servers or storage devices may be located in shared maintenance spaces as necessary, but whenever possible and in all new development shall be located in separate secure closets only accessible by IT. Access to existing closets should be limited to only staff who need to access these spaces for their job function at the college. These closets must be locked at all times.

3) **Portable Equipment**

The general recommendations for physical security are the same for all devices, particularly smaller devices like laptops, hard disks, smartphones, music players, and flash drives:

Never leave your laptop or small device unattended, even for a moment, even in your office. Most laptops are stolen from their owner's office, while the owner is at a quick break or meeting.

If you must leave your laptop in a car, you should stow your bag in the trunk. It is advisable to do this before you reach your destination, so potential thieves don't see you doing so. Make sure your car is locked.

Use a low-key shoulder bag, briefcase, or backpack for your laptop. Avoid expensive bags that scream, "Laptop inside!"

Do not leave portable electronic equipment unattended when traveling. Monitor it closely while checking in at an airport or hotel counter and while passing through airport security checkpoints. If you must leave the equipment briefly unattended in a hotel room, it should be secured to a desk or table with a cable lock or keep it in a hotel provided safe if available.

If you are going out for coffee or lunch, lock your gear in a desk or an office that can be locked. Or, at least purchase and use a laptop cable lock.

When traveling by air, bring the portable IT equipment with you on the airplane as a carry-on. Do not place it in checked luggage.

Portable devices should be configured to require a PIN or password to gain access to use the device.

USB flash drives or portable hard drives should not be used unless they are encrypted by the IT Department.

4) **Visitor Access**

All vendors or other visitors who need to have access to the data centers or networking closets must be escorted by IT, Security or other authorized staff. The visitor's names and purpose for being in the data center should be logged.

Vendors with extended ongoing maintenance and support contracts may be placed on an authorized visitor list and allowed by IT to check out keys from the Security office and to be able to access the data centers or network closets unescorted. They must sign out the keys and check them back in upon departing campus. Additionally, they must log in and out of the data center and state their purpose for their visit. If the contract with the vendor is discontinued, IT will notify security to remove the vendor from the authorized visitor list immediately, and no further access will be allowed.
A vendor who has authorized visitor access and do not need to be escorted, should carry ID on them and be prepared to identify who they are and why they are on campus.

Vendors who need access to IT resources in student rooms must be escorted at all times.

5) **Physical Protections**

Appropriate physical safeguards must be placed on equipment that stores or processes institutional data. In addition to physically securing this equipment, consideration must be given to other environmental related aspects that could, if not managed correctly, cause an interruption of service or availability and thus disrupt the university's mission. Careful thought must be given to ensure proper power (e.g., Uninterruptable Power Supplies, generator power backup, redundant power feeds), adequate Fire, humidity, smoke and temperature control systems, fire protection, protection against flooding and so on. These environmental safeguards must be commensurate with the sensitivity of the data contained in or processed by the equipment.