Weill Cornell Medicine

Service Policy

Devices: Computers

Responsible Executive: Chief Information Officer, WCM
Original Issued: November 3, 2016
Last Updated: March 12, 2020

Contents

1. Supported Computers

Supported computers are devices used by an individual (e.g., laptop, desktop, etc.) that are inventoried ("tagged") by ITS in order to connect to the Weill Cornell Medicine campus network.

1.01 Security for Supported Computers

Given the amount of data that can be stored on an individual's computer, security and management of the computer is paramount. ITS has developed a set of common standards and practices that must be adhered to when connecting any computer to the WCM network.

1.02 Minimum Security Requirements

Supported computers on the WCM network must adhere to the following minimum security requirements:

- Installation of computer management software (e.g., BigFix for Windows computers or Jamf for macOS computers)
- Installation of the ITS encryption software (in accordance with ITS policy 11.06 – Device Encryption)
- Installation of the ITS anti-virus/anti-malware software
- Use of a WCM CWID when logging in to a Windows computer
- Use of a strong, complex password when logging in to a macOS computer (in accordance with ITS policy 11.15 – Password Policy and Guidelines)
- Installation of critical security updates released by Microsoft or Apple
- Use of applications which still receive security updates released by the vendor
- Local administrator accounts will be renamed, disabled, or secured with a strong, complex password
- Services typically found on a server should not be installed on an individual's computer (e.g., web hosting services, routing or networking, etc.)

1.03 Administrative Access

Individuals with administrative access to their computers significantly increases the risk of infection from malware. Unless absolutely necessary, users should have 'standard' or non-privileged access to their computers.

2. Non-supported Computers

Non-supported computers are devices used by an individual (e.g., laptop, desktop, etc.) that are not inventoried ("un-tagged") and not managed by ITS that may be used to connect to the Weill Cornell Medicine campus network or store Weill Cornell Medicine data.

2.01 Security for Non-supported Computers

Non-supported computers must meet similar security requirements as tagged and managed computers. Given the amount of data that can be stored on an individual's computer and the risk an unmanaged device can pose to the Weill Cornell Medicine network, security of the computer is paramount. The following set of common standards and best practices must be adhered to for non-supported computers.

2.02 Minimum Security Requirements

Non-supported computers on the WCM network must adhere to the following minimum security requirements:

- Use of a modern operating system that regularly receive security updates from the manufacturer (e.g., no Windows XP, Windows 7, Windows 8, macOS Sierra, OS X El Capitan, OS X Yosemite, etc.)
- Installation of an anti-virus or anti-malware product that is current with definition or software updates
    - Windows 10 users may enable the built-in virus and threat protection in Windows Security
    - Many third-party products are available such as Norton, McAfee, or Sophos, among others. Your internet service provider may even provide these products at low or no additional cost.
- Installation of a host-based firewall product that is enabled and blocking uncommon connections
    - Windows 10 users may enable the built-in firewall in Windows Security
    - macOS users may enable the built-in firewall in System Preferences
- User accounts must be unique to the individual affiliated with Weill Cornell Medicine and configured with a strong password or passphrase
    - Individuals in a household that share the same computer must not have access to WCM data, applications, or services
- Critical security updates released by Microsoft or Apple must be installed

2.03 User Responsibilities

Individuals using a non-supported computer to access the Weill Cornell Medicine network are expected to comply with the above requirements and also complete the High Risk Attestation annually. Devices being used for long-term work purposes—including long-term storage of Weill Cornell Medicine data—should be tagged and encrypted by ITS in accordance with ITS policy 11.06 – Device Encryption.

2.04 Long-term Support for Non-supported Computers

ITS continually evaluates the risk of allowing non-supported computers to connect to the campus network and is balancing this need based on the availability of critical services and applications. In the future, non-supported computers may be limited in their ability to connect to the WCM network using remote access services such as VPN.

3. Non-standard Operating Systems

Computers connected to the WCM network that are not running an ITS standard operating system must adhere to the minimum security requirements identified above to the extent possible. Individuals with Linux-based devices, including Chromebooks, should limit access to web-based applications and services, only.