Weill Cornell Medicine

Service Policy

Devices: Support Computers

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

Contents

1. What are 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.

2. 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.

2.01 Minimum Security Requirements

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

- Installation of computer management software (e.g., Microsoft System Center Configuration Manager [SCCM]) for Windows computers or Jamf for Mac OS 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 Mac OS 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.)

2.02 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.

3. Non-standard Operating Systems

Computers connected to the WCM network that are not running an ITS standard operating system must still adhere to the minimum security requirements identified above.