

Windows Devices

Requirements

To be registered as compliant, all Windows devices must meet the following requirements:

- The device must be running a version of Windows still supported by Microsoft
- The device must require a password to be unlocked
- The device password must meet the following requirements (*these requirements apply only to non-company devices*):
 - o Password must be either a standard password or a numeric PIN
 - o Password must not be considered a “simple” password (e.g. sequential or repeated characters *abcdef* or *111111*)
 - o Password must be at least 6 characters in length
 - o Password must expire after a maximum of 730 days
 - o Password must be required after device returns from idle state (e.g. sleep or hibernation)
 - o Biometric (fingerprint/face recognition) login is not allowed under this policy.
- The data storage on the device must be encrypted with any full-disk encryption
- Antivirus and Antispyware software must be installed on the device, enabled, and up to date. Antivirus and Antispyware programs must be registered with Windows Security Center to be recognized (e.g. Symantec, Microsoft Defender, etc.). Microsoft Defender does meet this requirement.

Noncompliance

If an enrolled device does not meet the above requirements above for 21 days the following actions will be taken on the device:

- The device will be marked as noncompliant

Noncompliant devices will be prevented from using enterprise applications such as VPN, non-web-based Office apps (Word, Excel, PowerPoint, etc.), OneDrive, and other enterprise-managed apps, as well as being unable to connect to internal WiFi networks.