# Information Technology Policy

## *Windows 10 and 11 Configuration Requirements*

**Number**
OPD-PLT017A

**Effective Date**
February 26, 2016

**Category**
Platform

**Supersedes**
None

**Contact**
RA-ITCentral@pa.gov

**Scheduled Review**
September 2024

## 1. Purpose

This operating procedure document (OPD) provides guidance to agency IT administrators tasked with deployment of Windows operating systems. This document establishes the appropriate configurations that are required for deployment of Windows 10 and 11 operating systems.

## 2. Definitions

**Cortana** - A web enabled search function that uses Microsoft public cloud services to translate the search criteria and provide local and internet accessible results.

**Group Policy Objects (GPOs) -** A Microsoft Enterprise management capability for domain joined computers to apply specific configuration settings and restrict the user from the ability to change them.

**System Center Configuration Manager (SCCM)** – Systems management software for managing large groups of computers through remote control, patch management, software distribution, and operating system deployment.

**Telemetry** - The gathering of data points and environment parameters to be used for monitoring the endpoint devices. In this OPD, the Telemetry data collector is Microsoft.

## 3. Policy

Agencies that are deploying Windows 10 and 11 operating systems shall deploy the software with the configuration settings listed in Section 4.1 below.

Agencies shall comply with the product standards detailed in *ITP-PLT017C, Desktop and Laptop Operating System Standards.* These versions have the options required to disable the Telemetry data collection features that have been integrated into the

Windows 10 operating system.

Agencies that deploy non-compliant versions of Windows 10 and 11 operating systems risk having those devices with the non-compliant Windows 10 and 11 versions or configurations removed and/or blocked from Commonwealth IT resources.

Machines must be managed by the Enterprise SCCM site. This requirement is to further eliminate Telemetry data gathering.

## 3.1 Configuration Settings

The following configuration settings need to be applied and enforced using agency GPOs to all Windows 10 and 11 devices.

### 3.1.1 Disable Cortana

**Computer Configuration > Administrative Templates > Windows Components > Search**

- Allow Cortana: **Disabled**
- Allow search and Cortana to use location: **Disabled**

### 3.1.2 Disable Insider builds, Telemetry, and pre-release features

**Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds**

- Toggle User Control over Insider Builds: **Disabled**
- Allow Telemetry: **Enabled**
  - Option: **0 – Security [Enterprise Only]**
- Disable pre-release features or settings: **Disabled**
- Do not show feedback notifications: **Enabled**

### 3.1.3 Disable Automatic connecting and sharing WLAN info

**Computer Configuration > Administrative Templates > Network > WLAN Service > WLAN Settings**

- Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services: **Disabled**

### 3.1.4 Disable Microsoft Customer Experience Improvement Program

**Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication**

- Turn off Windows Customer Experience Improvement Program: **Enabled**

This chart contains a history of this publication's revisions.

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 02/26/2016 | Base Document |
| Revision | 11/24/2021 | Added third party vendors to Scope and Responsibilities Sections<br>Added Definitions<br>Removed McAfee VSE and HIPS<br>Updated Responsibilities and Exemption Section<br>Added links |
| Revision | 09/26/2023 | Updated to include Windows 10 and 11<br>Minor rewordings and clarifications<br>Removed Scope, Authority, Version Control, Exemption, and Reference sections as they are already covered in the ITP |