pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy Supporting Document

OPD-PLT017A – Windows 10 Configuration Requirements

ITP Number	**Effective Date**
OPD-PLT017A	February 26, 2016
Category	**Supersedes**
Platform	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	February 2017

1. Purpose

This operating procedures document 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 operating systems.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

3.1 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.

3.2 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.

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

3.4 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.

4. Policy

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

Agencies are required to comply with ITP-PLT017 *Desktop and Laptop Operating System Standards* Windows 10 product standards. These versions have the options required to disable the telemetry data collection features that have been integrated into the Windows 10 operating system.

Machines must be managed by an SCCM site running version 2012 SP2 or 2012 R2 SP1. This requirement is to further eliminate telemetry data gathering. SCCM 2007 does not support the required OS version.

Note: McAfee VSE 8.8 Patch 6 and McAfee HIPS 8.0 Patch 6 are supported for running on Windows 10.

4.1 Configuration Settings

The following configuration settings need to be applied and enforced using agency Group Policy Objects (GPOs) to all Windows 10 devices.

4.1.1 Disable Cortana

Computer Configuration > Administrative Templates > Windows Components > Search

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

4.1.2 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**

4.1.3 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**

4.1.4 Disable Microsoft Customer Experience Improvement Program

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

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

5. Responsibilities

5.1 Office of Administration, Office for Information Technology (OA/OIT)

Office of Administration, Office for Information Technology (OA/OIT) will perform testing for support of enterprise applications and services and provide agencies with the testing results. When enterprise applications and services are validated to be compatible with Windows 10, agencies will be notified through proper communication channels.

5.2 Commonwealth Agencies

Commonwealth Agencies will deploy Windows 10 operating systems with the required configurations stated in this operating procedures document to their internal agency devices. The agencies are responsible for revising and updating operating system configurations as required by ITP-PLT017 *Desktop and Laptop Operating System Standards* and this operating procedures document.

6. Related ITPs/Other References

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-PLT017 – *Desktop and Laptop Operating System Standards*
- ITP-BUS004 – *IT Waiver Review Process*
- *ITP-SYM006 - Desktop and Server Software Patching Policy*

7. Authority

Executive Order 2011-05, Enterprise Information Technology Governance

8. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

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

Version	Date	Purpose of Revision
Original	02/26/2016	Base Document