Information Technology Services

ITS Tier 0, 1, & 2 Software Baseline Standards

Author(s):	Bill Rivers
Date:	11/04/2021
Version:	2.0

Washington State University

Revision History

Version No.	Date	Description	Author
1.0	11/04/2021	Initial Release	Bill Rivers
2.0	01/07/2022	Added MAC, Linux, Creative Cloud	Garrett/Movius/Allen/Jacobs

Reviewed By:

DocuSigned by:

1/13/2022

A655BDB60CF742C...

Michael Walters, Interim CISO — Date

DocuSigned by:

Carrie K Johnson

1/13/2022

D7C04E5F5955420...

Carrie Johnson, Interim Assistant Vice President, Administrative & Financial Services — Date

DocuSigned by:

Darren Michael Yocum

1/14/2022

51CCA7434C0F432...

Darren Michael Yocum, Assistant Vice President — Date

DocuSigned by:

Tony Opheim

1/14/2022

97CA1EF90EE840A...

Tony Opheim, Associate VP & Deputy CIO — Date

Approvals

DocuSigned by:

Sasi Kumar Pillay

1/20/2022

8201AF15A292449...

Sasi Pillay Ph.D., Vice President and CIO — Date

Contents

1. Introduction

ITS maintains a standard list of applications for base installs on Tier 0, Tier 1, and Tier 2 systems. This list is actively maintained with up to date software versions and is used as the base image installation for new systems. SCCM, Ansible and Intune are used as the tools for software compliance and systems of record for each operating system.

2. Purpose

Define a standard to ensure proper software is maintained on managed systems. These requirements apply to Tier 0, Tier 1, and Tier 2 systems managed by Central ITS.

3. Scope

Develop standard for managing software inventory on server and desktop/laptop systems:

- Define baseline standard
- Define reporting requirements
- Define technical and exception requirements

4. Effective Dates

This standard is effective immediately upon date of approval by the CIO.

5. Roles and Responsibilities

ITS system administrators will ensure these ITS standards are implemented on ITS managed software installations and ongoing version maintenance will be maintained.

6. Baseline Standard

ITS maintains a standard list of required baseline software to be installed and managed on ITS owned systems. This list includes both security and business software as needed. Software is assigned based upon the system involved (i.e., Tier 0, Tier 1, and Tier 2 systems) but are all managed using the tool set(s) identified below.

6.1. ITS T0/T1 Baseline Image & Monitoring Standard

ITS uses configuration management tools to deploy and monitor baseline image configurations for compliance and deviations.

- ITS deploys Windows Security and Critical updates to all WSU T1/T0 servers and workstations every 30 days. ITS installs T1 updates to ITS servers within a 7-day period after deployment. Users of WSU T1 workstations have 7 days to install the patches before they are forced to install. WSU T0 workstations are forced to install 2 days after deployment. Compliance is monitored using SCCM.

- ITS deploys the anti-virus/anti-malware application Cortex XDR via SCCM to all ITS T1/T0 servers and workstations. We monitor compliance in SCCM, and summarization is run every 7 days.

- To monitor the Windows version and base image software installations/deviations for ITS T1/T0 servers and workstations, we use SCCM to deploy ITS created image baselines.

- Production Linux systems are patched monthly and development systems weekly.

- Cortex XDR is deployed to all Linux systems.

- Installed software on Linux machines is managed in Ansible playbooks.

ITS Monitored T0/T1 Server & Workstation Software Baseline

Below are the current baselines that are monitored and defined in System Center Configuration Manager (SCCM) or Ansible:

- Supported operating system
- Cortex XDR
- Splunk Universal Forwarder
- LAPS – Local Administrator Password Solution (Windows machines only)
- Palo Alto Global Protect VPN Client (workstations only)

6.2. ITS T2 Baseline Image Monitoring Standard

ITS uses Microsoft System Center Configuration Manager (SCCM) and Intune to deploy and monitor our baseline endpoint image and for compliance with and deviations from this baseline.

- ITS deploys Windows Security and Critical updates to all ITS T2 machines every 30 days, and the user is given 3 days to install before the update is forcibly installed. Compliance is monitored and we use the Deployments Monitoring tool in SCCM and as well as Intune to monitor all ITS T2 Workstations.

- To monitor Malware on ITS T2 machines we deploy Endpoint Protection to all ITS workstations in SCCM. Viruses and Malware is detected using Cortex XDR and Malwarebytes. Alerts and infections automatically open a ticket with Endpoint Support with the action taken. If the action was successful, we move the ticket to the Operational Notification area in Jira. If the action was not successful, then the machine will be taken off the network and the machine reimaged.

- ITS deploys BitLocker drive encryption to all ITS T2 Windows laptops. To monitor BitLocker compliance on ITS laptops we deploy BitLocker enabled on Mobile Devices baseline to our ITS – ITS Laptops collection and summarization is run every 7 days.

- ITS deploys the anti-virus application Cortex XDR to all ITS T2 machines. We monitor compliance on all ITS T2 machines and summarization is run every 7 days.

- The ITS- T2 Windows Configuration Baseline is deployed to all ITS machines and summarization is run every 7 days. This monitors the Windows version and base image software installations and any deviations discovered.

<u>ITS Monitored Tier 2 Software Configuration</u>

Windows T2:

Windows 10 Enterprise (or above) – Operating System

Office 365 - Productivity

Splunk - Security

Cortex XDR - Security

Global Protect - Security

Malwarebytes - Security

LAPS – Local Administrator Password Solution - Security

Chrome – Web Browser

Zoom – Productivity

Creative Cloud - Productivity

Company Portal (Intune)

MacOS T2:

MacOS Catalina or higher – Operating System

Cortex – Security

Splunk - Security

Malwarebytes – Security

Office 365 – Productivity

Zoom – Productivity

Global Protect – Security

Creative Cloud - Productivity

Company Portal (Intune)

7. Reporting

As outlined in the sections above SCCM, Ansible and Intune are utilized to ensure the correct software is installed and is running the current version. Reports can be run as requested.

8. Exceptions Requirement

All exceptions require the approval of the CISO and DCIO and are managed through the ITS Exception Policy and Process.

9. Review Cycle

This policy will be reviewed and updated as required.