# VA STANDARD DESKTOP CONFIGURATIONS

1. **REASON FOR ISSUE**: To revise the Department of Veterans Affairs (VA) policy on standard desktop configurations. This directive establishes a process for defining a VA-wide enterprise software suite and a range of acceptable hardware configurations, and how that information will be published. It also establishes a four-year refresh cycle for all laptops and desktop computers. This directive does not apply to thin-client devices, or IOS devices. Use of these devices will be considered on a project by project basis as part of the standard Information Technology (IT) project oversight process.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES**: This directive sets forth the policies and responsibilities for implementing and complying with VA Baseline Configurations, hereinafter referred to, as “baseline”. The directive contains:

   a. A definition of the VA-wide corporate software suite and a range of acceptable hardware configurations. Specifics of the software suite will be maintained by The Office of Information and Technology (OIT), Development, Security, and Operations (DevSecOps) and acceptable hardware configurations will be maintained by OIT Office of Strategic Sourcing (OSS).

   b. A definition of the responsibility for all VA facilities to develop plans to implement a four-year refresh cycle for all laptops and desktops.

   c. Significant changes to this directive include:

      (1) Updates to reflect the current fiscal and operational environment.

      (2) Exceptions for this directive are not allowed. Non-compliance with standard desktop configurations will be addressed via a Plan of Action and Milestones (POA&M) in the Governance, Risk and Compliance (GRC) tool.

3. **RESPONSIBLE OFFICE**: Office of Information and Technology (OIT), Development, Security and Operations (DevSecOps).

4. **RELATED HANDBOOK**: None.

5. **RESCISSION**: VA Directive 6401, VA Standard Desktop Configurations dated June 24, 2002.

**Department of Veterans Affairs**
**Washington, DC 20420**

**VA DIRECTIVE 6401**
**Transmittal Sheet**
**June 8, 2021**

**CERTIFIED BY:**

/s/
Dat P. Tran
Acting Assistant Secretary for
Enterprise Integration

**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:**

/s/
Dominic A. Cussatt, CGEIT, CISM
Acting Assistant Secretary for
Information and Technology and
Chief Information Officer

**DISTRIBUTION**: Electronic only

# VA STANDARD DESKTOP CONFIGURATIONS

## 1. PURPOSE.

a. This directive establishes a four-year technology refresh cycle for all Windows based laptops and desktops, to optimize and maintain the baseline environment and to facilitate management of the VA IT portfolio. It also establishes a method for developing and publishing standard baselines, made up of hardware, security settings, other settings and software for Window based laptops and desktops throughout VA

b. VA has various hardware and software configurations for Windows-based laptops and desktops throughout VA organizations. Standardization reduces the complexity of designing and implementing centralized systems and standardized settings including security policies. In addition, hardware is procured with various technology refresh cycles, with some upgraded every year and others upgraded based on a specific project need.

## 2. POLICY.

### a. Standard Software Configuration

(1) The VA Enterprise office automation software suite will be developed consistent with the VA Enterprise Architecture and other IT strategic documents. The VA Enterprise Windows baseline software suite considers the environment at the VA Enterprise level to include a standard operating system, suites of office automation software, corporate anti-virus, firewall, universal serial bus (USB) device control and forensic auditing software products, one or more terminal emulation packages to interface with VA legacy systems, and any other client software packages deemed necessary for VA enterprise wide need.

(2) The corporate office automation software suite will always consist of commercial off-the-shelf products. The published corporate office automation software suite, maintained by DevSecOps, will include only products available for purchase, not beta or pre-release versions of software, unless there are compelling business needs.

(3) The specific components of the corporate office automation software suite will be approved by the VA Technical Reference Model (TRM) based upon recommendations from architecture, engineering, lifecycle management, security and other pertinent groups. The TRM is the official list of approved corporate software. These components will be reviewed annually and updated if necessary. Information System Owners (ISOs) must ensure all TRM approved installed software is part of a valid Authority To Operate (ATO) boundary.

(4) Software packages procured by business lines (e.g., Veterans Benefit Administration (VBA), Veterans Health Administration (VHA), National

Cemetery Administration (NCA), Office of Electronic Health Record Modernization (OEHRM), etc.) to augment the office automation suite must have client interfaces compatible with the VA corporate office automation suite and comply with the baseline settings without change, so that it is unnecessary to purchase additional hardware or to violate standard configurations to support them.

**b. Standard Hardware Configurations**

(1) Subject to operational and budgetary constraints, VA baseline laptops and desktops must be upgraded every four years to ensure that they will be able to process the latest versions of office automation software and that they are suitable for newly developed VA-wide business-line systems. Therefore, OIT will develop the necessary plans and procedures to ensure that all baseline laptops and desktops are upgraded or replaced to meet the requirements of this directive every four years. Funding these upgrades or replacements shall be completed consistent with Directive 6008, Acquisition and Management of VA Information Technology Resources.

The VA CIO, based on the recommendations of architecture, engineering, lifecycle management and other pertinent groups, will establish standard offerings of laptops and desktops utilizing Office of Management and Budget (OMB) guidance which recommends a base configuration with upgrade options based upon customer requirements. Per OMB guidance provided in Memo M-16-02, Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops, the VA shall ensure that at least 80 percent of new basic laptop and desktop requirements are to be satisfied by one of the standard configurations offered through consolidated acquisition opportunities meeting Federal Information Technology Acquisition Reform Act (FITARA) implementation guidelines.

(2) The hardware configurations governed by OIT DevSecOps are minimum requirements and are updated on a quarterly basis. Supervisors and managers may add additional peripherals, additional storage space or memory based on local needs. In addition, adaptive peripherals or software may be provided as a reasonable accommodation if the designated user of the laptop and desktop has a special need (e.g. equipment to accommodate a disability or physical space, etc.). Please note that any additional peripherals must be compatible with the VA corporate baseline and office automation software suite and the defined hardware configurations or they must be removed from the device.

**c. Baseline Non-Compliance and POA&M**

(1) Exceptions to this Directive are not allowed. Non-compliance is defined as systems that cannot fully comply with approved Enterprise Secure

Configuration Baselines. OIT will officially document non-compliance through POA&Ms, which will capture, at the very least, the reason for the non-compliance and track mitigation efforts. The POA&M will be reviewed and accepted by the CIO, or designee.

(2) The Information System Owner, or system steward, will create a POA&M item to track mitigation efforts. The documentation for non-compliance should include business reasons, risk analysis and any mitigating or risk reducing factors.

(3) Information System Owner or designee must present the non-compliant baseline to the appropriate change advisory board for approval via the change order process.

**d. Security**

(1) A security standard for VA baselines is established within the specification of hardware and software and is a part of each baseline. The security standard is in accordance with Configuration Management (CM-2), Baseline Configuration, Knowledge Service Security Controls, and Defense Information Systems Administration (DISA) Security Technical Implementation Guides (STIGs). This security standard must be implemented on each VA baseline.

(2) All VA baseline equipment scheduled to be removed from service (surplus to Government needs, transferred to another organization not considered under contract or oversight of VA, discontinued from rental/lease, exchanged, sold, or otherwise released) must be in accordance with and adhere to Media Protection (MP-6), Media Sanitization, Knowledge Service Security Controls. Devices may be transferred between VA or trusted partner or vendor locations by VA staff, contractors or commercial carriers to meet mission needs provided storage media adheres to the guidance in Media Protection (MP-5), Media Transport/ Cryptographic Protection, Knowledge Service Security Controls.

## 3. RESPONSIBILITIES.

a. **Assistant Secretary for Information and Technology and CIO**. The CIO is the senior agency official responsible for the Department's IT programs and is responsible for ensuring compliance with the VA Baselines. The CIO will review and evaluate compliance with this directive.

b. **Under Secretaries, Assistant Secretaries, and Other Key Officials** shall ensure compliance with this directive within their respective Administrations and Staff Offices, to include:

(1) Ensuring all centrally and/or business line procured or developed software developed for administrative and office automation purposes is compatible with the VA corporate office automation software suite and baseline settings.

(2) Ensuring that information systems owner or system stewards take necessary steps are taken to submit a POA&M for any deviations from the standard laptop and desktop configuration.

c. **Deputy Assistant Secretary, DevSecOps** has operational responsibility for this directive, to include:

(1) Maintaining the specific components of the corporate baseline and office automation suite and the hardware configurations are published and ensuring updates are completed as required; and

(2) Ensuring implementation plans are developed as necessary to ensure that all baseline laptops and desktops are upgraded at least once every four years.

d. **ISOs** are responsible for

(1) Ensuring all system changes are accurately reflected in the Governance, Risk and Compliance (GRC) tool. VA ATO packets with a "Significant/Major Change" as identified in the eMASS Authorization Requirement SOP Guide must be re-evaluated by the Authorizing Official (AO) based on the National Institute of Standards and Technology (NIST) 800-53 guidelines and VA Policy. Use the Knowledge Service, eMASS as a reference.

(2) Ensuring all loaded software, TRM-approved or otherwise, is documented within the ATO boundary.

**e. Deputy Chief Information Officer (DCIO), OSS** is responsible for ensuring a list of acceptable hardware configurations is maintained.

## 4. REFERENCES.

a. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program published March 10, 2015.

b. Knowledge Service, Security Controls

c. VA Directive 6008, Acquisition and Management of VA Information Technology Resources published November 2, 2017.

d. Federal Information Technology Acquisition Reform Act passed by Congress December 19, 2014.

e. OMB Memo M-16-02, Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops, published on October 16, 2015.

f. VA Handbook 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems published February 3, 2014.

g. eMASS Authorization Requirement SOP Guide published January 13, 2021.

h. Knowledge Service eMASS