VIRGINIA IT AGENCY

Commonwealth of Virginia

Enterprise Solution Architecture [ESA]

Smart Device Use

COV & Bring Your Own Device

vita.virginia.gov

February 1. 2022

Revision History

Smart Device Use: Version History		
Revision	**Date**	**Description**
1.0	06/24/2021	Original. This document was derived from the *Mobile Communications Use Technical Topic Report*, which has been rescinded.
	08/03/2021	Revised per comments from Mike Watson, consultation with JB Edmonds.
	10/29/2921	Revised per comments from EA, SA.
	02/01/2022	Revised per comments from ORCA.
1.0a	02/01/2022	Added administrative note to SDU-11

Review Process

This requirements document was posted on VITA's Online Review and Comment application (ORCA). All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were evaluated and Individual commenters were notified of action(s) taken.

Requirements & Agency Exceptions

The requirements included within this document are mandatory. Agencies deviating from these requirements must request an exception for each desired deviation, and receive an approved E*nterprise Architecture Exception* via Archer, prior to developing, procuring, or deploying such technology, or not complying with a requirement specified in this document. The instructions for completing and submitting an exception request are contained within the *Commonwealth Enterprise Architecture Policy*.

Contents

Scope

The requirements for the use of smart devices supports the ability for state employees to use personal devices to access commonwealth voice and messaging systems while conducting official state business. Institutions of higher education are excluded from these requirements, but are encouraged to consider the provisions included herein when developing internal smart device use policies.

Smart Device Use Vision and Strategy
Vision
Smart devices offer new ways for organizations to solve daily business functions by transforming how employees collaborate. The growing diversity of smart device form factors, and the vendors that supply them, offer a variety of choices for how an organization may elect to address these functions. The inclusion of smart devices in the toolsets available to COV employees will greatly enhance COV's ability to conduct state business.
Strategy
Objective 1: Define what is a COV Smart Device Objective 2: Identify the constraints under which smart devices may be used Objective 3: Identify the requirements for smart device management Objective 4: Identify the rules for BYOD smart devices

Purpose

The intent of these requirements is to govern the purchase, design, implementation, and on-going operation of COV IT services and utilized technologies. For further information on the perspectives, please reference the most recent version of the Enterprise Solutions Architecture (ESA) Requirements document.

Definitions and Terminology

Bring Your Own Device (BYOD)	A practice whereby an organization permits employees to use personally owned smart devices to conduct business, rather than being required to use an employer-provided device. Also called Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP), and Bring Your Own Personal Computer (BYOPC).
BYOD Smart Device	Any personally owned smart device that is used to connect to a COV network, or to another smart device authenticated to a COV network, which • Can store COV data • Can be managed through MDM • Has been authorized by an agency for a COV employee
COV Data	Data maintained, transformed or stored by an agency or its designee in the performance of Commonwealth business.

COV-Registered Phone	A personally owned phone registered with VCCC for serving as the second factor in a two-factor authentication transaction. A registered phone may be any device capable of receiving phone calls, including smartphones, call-only mobile phones, or landline phones. The phone is not necessarily a BYOD smart device, but may be used as one if it meets the definition.
COV Smart Device	Any COV purchased smart device that is used to connect to a COV network, or to another smart device authenticated to a COV network, which • Can store COV data • Can be managed through MDM • Has been issued and authorized by an agency for a COV employee
Form Factor	A hardware design aspect that defines and prescribes the size, shape, and other physical specifications of components, particularly in electronics. Examples of different smart device form factors include: • Laptops • Smartphones • Tablets
Mobile Application Management (MAM)	Software responsible for provisioning and controlling access to business apps used on smart devices, on both company-provided and BYOD mobile operating systems.
Mobile Device Management (MDM)	Software that allows IT administrators to control, secure and enforce policies on smart devices.
Smart Device	An electronic device capable of connecting to a network, or to other devices, via wireless communication protocols, and which can operate interactively and autonomously to some extent. It includes devices that exhibit some properties of ubiquitous computing, such as artificial intelligence. Smart devices support a variety of form factors, a range of properties pertaining to ubiquitous computing and to be used in three main system environments: physical world, human-centered environments and distributed computing environments. Several notable types of smart devices are: • Laptops • Smartphones • Tablets & Phablets • Smartwatches • Smart bands • Smart vehicles

Smartphone	A class of smart devices that combines cellular and mobile computing functions into one unit. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging. Smartphones typically contain a number of metal–oxide–semiconductor (MOS) integrated circuit (IC) chips, include various sensors that can be leveraged by pre-included and third-party software (such as a magnetometer, proximity sensors, barometer, gyroscope, accelerometer and more), and support wireless communication protocols such as Bluetooth, Wi-Fi, or satellite navigation.
Wireless Communication	The transfer of information between two or more points that does not use an electrical conductor as a medium by which to perform the transfer. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of applications of radio wireless technology include GPS units, garage door openers, wireless computer mouse, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones. As of this publication, current wireless communication protocols include: • 3G/4G/5G Cellular • 6LoWPAN • ANT & ANT+ • Bluetooth & Bluetooth Low Energy (BLE) • Dash7 • DigiMesh • EnOcean • Ingenu • Li-Fi • LTE Cat-M1 • LoRaWAN • mcThings • MiWi • NFC • NarrowBand-IoT • RFID • SigFox • Thread • WirelessHART • Weightless N/P/W • Wi-Fi • Wi-Fi-ah (HaLow) • Z-Wave • ZigBee

Scope

These requirements address the use of smart devices employed to conduct official business of the Commonwealth of Virginia (COV), and covers both COV and BYOD smart devices used by Executive branch agencies. This document focuses primarily on the rules for smart device use, rather than on the application software that may be deployed on the device. The governing roadmaps for smart devices include:

- End User Compute Operating System Technologies Roadmap
- End User Compute Web Browsers Technologies Roadmap
- End User Compute Productivity Software Technologies Roadmap

These and related documents are located in the EA Library.

There are eight perspectives addressed in this document:

1. Solution Business Requirements
2. Design/Architecture
3. Availability/Performance
4. Capacity
5. Continuity
6. Integration/Interoperability
7. Technology
8. Security

Solution Business Requirements

General Provisions

SDU-01 COV smart device services shall support COV and BYOD smart devices.

- COV smart device services shall include management of COV and BYOD smart device compliance
- COV smart device services shall have a sparing strategy of device reserves to a minimum of 2% of the customer base
- COV smart device services shall ship replacement or spare COV smart devices within 2 days, and deliver to the hands of the end user within 5 days
- COV smart device services shall provide replacement for unrepairable COV smart devices
- COV smart device services shall either complete repair of COV smart devices within ten business days of reporting or replace them
- COV smart device services shall provide back-up devices to COV smart device customers for the period in which a device is being repaired.

SDU-02 Suppliers of COV smart device services shall notify VITA, customers, and third parties involved in the delivery, or affected by mass outages hindering functionality of COV smart devices within an hour of detection.

SDU-03 The identification, selection, and acquisition of COV smart device service plans is centrally managed by VITA. VITA shall provide agencies with the means to:

- Review of smart device use and related costs
- Review of smart device plans processes to manage, monitor, and control the costs

Agency Smart Device Use Policies

SDU-04 Agencies shall develop a policy for agency smart device use. Agency provisions may be more restrictive than the provisions herein, but may not be less restrictive.

SDU-05 Agencies shall document their policy describing use or restriction of smart devices. The policy will at a minimum:

- Establish the criteria for which positions in that agency require the provision of a COV smart device
- Establish the criteria and who has the authority to request an employee to surrender a COV smart device to Commonwealth Security for review and forensic imaging.
- Establish criteria for the network connectivity services needed to support the smart devices

SDU-06 The agency ISO shall ensure that a current inventory of the smart devices used by the agency is maintained. At a minimum, the inventory shall include a serial and/or IMEI number, a description of each device, the primary network connectivity for each device (i.e. ATT network, Verizon Network, Wifi, etc.) and the individual to whom the device is issued.

SDU-07 Agencies shall define processes for the review of smart device use and related costs. This review should occur annually.

- Ensure compliance with the agency policy of ongoing individual and agency-wide business justification and plan usage effectiveness
- Who is utilizing those services, and if the devices are being used as intended
- Saturation of BYOD versus purchased devices
- Volume of stolen and break fix devices

SDU-08 Agencies shall define processes for the review of smart device plans processes to manage, monitor, and control the costs. This review should occur annually.

- Review COV provided devices for consumption of minutes and data
- Identify capacity issues, such as if plan use is within 10% of available minutes
- Review changes in connectivity coverage that will affect agency employees

SDU-09 In order for an employee to be authorized for more than a single class of smart device, approval shall be documented and approved by the agency head or designee.

Note An employee may be issued a laptop and smartphone, but not two smartphones, without approval.

SDU-10 Agencies shall have an on-boarding and off-boarding process and policy for smart devices. The policy shall include the following:

- The agency will withhold the value of the COV smart device from the employee's pay if not returned upon request or termination
- All records relating to commonwealth business are considered to be Commonwealth data, even though generated on a BYOD smart device
- State business records are subject to review and disclosure unless the Freedom of Information Act (FOIA) permits or requires them to be withheld.

- The COV smart device user must agree to surrender the device to Commonwealth Security for review and forensic imaging per the agency smart device use policy
- The smart device user must agree to surrender the device to Commonwealth Security for review and forensic imaging per the agency smart device use policy
- In order to provide a stipend to an employee authorized to use a BYOD smart device, the COV Mobile Device Allowance Agreement shall be completed and signed.

SDU-11 Once a device is identified as no longer authorized for use (i.e. employee separation, device decommission), all Commonwealth data and services must be removed from the device and any associated storage or devices within 48 hours.

Note Storage may include any employed device storage, such as a SIM card, or cloud-based locations.

Note Any porting of telephone number requests after the decommissioning of a COV procured device will be addressed on a case-by-case basis

SDU-12 The service supplier, in coordination with VITA, shall document and maintain a smart device baseline configuration, which shall clearly identify any special security considerations and operational requirements for smart devices. This baseline configuration shall include:

- Configurations for protecting agency data and resources on the device
- Features of the device not authorized for use

Smart Devices

SDU-13 Selection of COV smart device service plans shall consider the role of the employee to whom it will be assigned and the potential extent of use when determining the number of minutes, SMS messages, and data download.

SDU-14 Where COV smart devices are subject to harsh usage conditions, such as strong vibrations, extreme temperatures above 100 degrees, or work around more than 6 inches of water longer than an average of two hours a day, the agency shall consider utilizing ruggedized devices that meet the Ingress Protection Code (IP Code) IP67 or IP68, and higher quality protective cases.

- IP Code 6–Dust-tight. No ingress of dust; complete protection against contact.
- IP Code 7–Immersion, up to 1 meter (3 ft 3 in) depth. Ingress of water in harmful quantity shall not be possible when the enclosure is immersed in water under defined conditions of pressure and time (up to 1 meter (3 ft 3 in) of submersion).
- IP Code 8– Immersion, 1 meter (3 ft 3 in) or more depth. The equipment is suitable for continuous immersion in water under conditions, which shall be specified by the manufacturer. However, with certain types of equipment, it can mean that water can enter but only in such a manner that it produces no harmful effects.

Smart Device Use Agreement

SDU-15 If the agency permits the use of smart devices, the agency smart device policy shall include a *Smart Device Use Agreement* that contains statements for the following:

- That each employee authorized to use a COV smart device is responsible for the reasonable care and due diligence in using, handling and protecting devices that access, receive, transmit, store or manipulate commonwealth data or information.

  Note If the device has a case or cover it is expected that it be used.
- That employees shall take reasonable precautions to protect COV smart devices assigned to them from damage, loss, theft, fraud or other misuse. Devices shall not be left unattended or unsecured.
- That except where prohibited by law, employees do not have, and shall not expect, privacy while using any COV smart device. This includes but is not limited to usage detail information; telephone numbers dialed and received; data transmission content and email, chat, data maintained on the smart device and notifications.
- That limited personal use of COV smart devices shall be permitted as long as it does not materially or routinely affect the cost or operation of the smart device.

  Note The agency shall consider the position and the job function of the user when determining incidental personal use. As an example, a position requiring overnight travel might be permitted to call home from the COV smart device while traveling.
- That employees using authorized BYOD devices acknowledge acceptance of agency and commonwealth policies and authorized Commonwealth personnel may access standards as well as the underlying data on the device.

BYOD Smart Devices

SDU-16 Each agency shall include in their policies the criteria under which BYOD smart devices will be permitted.

SDU-17 Jailbroken/rooted devices will not be authorized to be used as BYOD smart devices.

SDU-18 When approving BYOD smart devices, agencies shall ensure the capabilities of the device meet the intended use.

Note Some devices may be used for simple voice calls and email access, but may not be appropriate for running smart device applications, which require specific operating systems, memory/processor requirements, or other application-specific configurations.

SDU-19 Agencies may elect to provide a stipend to reimburse employees authorized to use BYOD smart devices for commonwealth business up to a maximum of $45. The agency is responsible for the cost of services for both BYOD and COV smart devices.

SDU-20 Agencies shall only offer a stipend or reimbursement to an authorized user for a maximum of one assigned smart device.

SDU-21 Agencies that elect to provide stipends to reimburse employees for use of a BYOD smart device shall comply with the Department of Accounts CAPP Manual.

Reimbursement for BYOD Smart Devices

The Department of Accounts (DOA) has established provisions in the Commonwealth Accounting Policies and Procedures (CAPP) Manual that govern the terms under which agencies may provide

stipends to employees as reimbursements for the use of BYOD smart devices to conduct official business. The DOA policy establishes how the maximum allowed reimbursement shall be applied in order for the stipend to be provided in compliance with commonwealth policies and federal Internal Revenue Service (IRS) income tax and withholding laws.

SDU-22 The maximum allowed reimbursement shall be $45.00 per month.

SDU-23 Reimbursements shall only be offered to employees who provide approved smart devices that are provisioned to support voice and data, or data-only functions. Cellular telephones and other devices that only support voice and text messaging are not capable of or not configured to, at minimum, receive commonwealth email messages are not eligible for a stipend or reimbursement.

SDU-24 Employees or authorized users shall normally only be authorized a single stipend for single non- commonwealth owned smart device. The agency head or designee may grant exceptions to this provision. Documentation of the exception and its justification shall be retained in the agency's files for the duration the exception is in effect and/or audit, whichever is later.

Design/Architecture

SDU-25 COV smart devices shall comply with COV technology roadmaps. Any device lacking a roadmap must have an approved EA exception prior to ordering and use.

SDU-26 COV and BYOD smart devices used to conduct official business and store commonwealth data must support the following capabilities:

- Support separation of commonwealth data from personal data on the device via containerization, whereby a portion of the device can be segregated into a protected area secured by a separate password and regulated by a separate set of policies in order to protect the COV network
- Support an approved MDM technology
- Support the ability to run one or more approved smart device codebases
- Maintain the approved smart device configuration baseline

SDU-27 COV smart devices shall integrate across COV supported form factors, such that they seamlessly interact with each other while leveraging their native capabilities in a way where they do not require additional configuration or administration.

- Virtual drives can create and open content for applications within the smart device suite
- Applications can embed and open content from other applications within the smart device suite
- Event artifacts such as notifications or meeting acceptances are presented through existing applications within the smart device suite

Availability/Performance

SDU-28 Agencies shall select a COV smart device service plan that supports a minimum download speed of 30Mbit/s or greater.

SDU-29 When purchasing COV smart devices that connect to cellular networks, agencies shall prefer unlocked devices that can switch between cellular networks.

Capacity

SDU-30 COV smart devices shall support data consumption of at least 30 Mbps or greater.

Note

- 3g = 4 Mbps
- 4g+ = 30 Mbps
- 5g = 150 Mbps

SDU-31 Selection of a COV smart device for a user shall consider the intended use of the device with respect to storage for applications and COV data.

- Smartphones and tablets shall have at least 64 GBs
- Laptops shall have at least 128 GBs

Continuity

SDU-32 Suppliers of COV smart device services shall provide capability to retain select content on a device in the event of a MDM services or network outage.

SDU-33 COV smart devices shall be configured such that primary storage of COV accessed by the device is not exclusive to the device, and that such data is stored in more than one location.

Integration/Interoperability

SDU-34: Suppliers of COV smart device services shall integrate with common industry smartphone and tablet devices.

Note Examples include, but are not limited to Apple iPhones and iPads, or the Samsung Galaxy S and Note.

SDU-35: COV smart device services shall integrate with COV MDM and MAM services.

SDU-36: COV smart device services shall support synchronization of data to smart devices, including:

- Email
- Attachments
- Address book
- Task list
- Chat
- Calendar

SDU-37: COV smart devices shall comply with requirements defined in EA Solution End User Compute Device Requirements.

SDU-38: COV smart devices shall comply with technology requirements defined in EA Solution Messaging Service Requirements.

Technology

SDU-39 Bluetooth-capable COV smart devices shall at a minimum support Bluetooth 5.0.

SDU-40 Wi-Fi-capable COV smart devices shall at a minimum support:

- Wi-Fi 5 (IEEE 802.11 ac, 802.11 ad, or both)

- Dual band (2.4 and 5 GHz)

SDU-41 Wi-Fi-capable COV smart devices that support Wi-Fi 6E shall also support 2.4 GHz and 5 GHz frequencies.

SDU-42 Suppliers of COV smart device services shall provide end-to-end diagnostics for the device, its software, and connectivity faults.

SDU-43 Suppliers of COV smart device services shall provide end-to-end support for such devices for users, including device setup and configuration.

SDU-44 Suppliers of COV smart device services shall ensure that the device operating system and applications are patched and upgraded appropriately, so that their versions are either the current release (*n*) or the prior release (*n-1*) per the COV technology roadmaps.

SDU-45 Suppliers of COV smart device services shall manage the Mobile Device Management (MDM) tool in accordance with VITA Rules.

SDU-46 Suppliers of COV Mobile Device Management (MDM) shall provide services and features typical of enterprise MDM services in the market, including, but not limited to:

- Web content filtering
- Access to multiple mailboxes
- Operate on common industry smart devices
- Multi-tenant application distribution
- Application packaging
- Over-the-air provisioning
- Policy management
- Associated reporting
- Device decommissioning

SDU-47 COV and BYOD smart devices shall be configured to routinely synchronize with the COV MDM solution in order to maintain their currency.

SDU-48 Suppliers of COV MDM services shall identify COV or BYOD smart devices that have not synchronized with the MDM solution after 48 hours and unenroll such devices.

SDU-49 COV smart devices shall support location sharing via GPS or mobile network triangulation.

SDU-50 Suppliers of COV MDM services shall distribute and install recommended operating system and application updates automatically.

SDU-51 Suppliers of COV MDM services shall notify end users of the need to initiate an update where automatic updates are not possible via COV email.

SDU-52 Suppliers of COV MDM services shall provide user documentation and support for the update process at a shared location available to VITA, the agencies, and other COV suppliers.

SDU-53 Suppliers of COV Mobile Application Management (MAM) services shall provide services and features typical of enterprise MAM services in the market, including, but not limited to:

- Application delivery in the form of an enterprise application store as well as a multi-tenant application store

- Application updating with new revisions
- Application version management
- Application configuration management by policy
- Application pushing
- Application event management
- Application wrapping and deployment
- Application packaging for deployment
- Device content retention in the event of a MAM services or network outage
- Multi-tenant application distribution
- Over-the-air provisioning
- Application crash log reporting
- Application reporting and tracking
- Usage analytics

SDU-54 Suppliers of COV smart device services shall support the existing COV MAM infrastructure, including all hardware, software, and tools necessary to support its operation.

SDU-55 COV smart devices shall be configured so that they will switch to Wi-Fi for internet connectivity when in proximity to a COV network.

Security

SDU-56 All smart devices shall be configured to meet commonwealth security policies and requirements as defined in:

- IT Information Security Policy (SEC 519-00)
- IT Risk Management Standard (SEC520-02)
- IT Security Audit Standard (SEC502-04)
- IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511-00.2)
- SEC501 Information Security Standard
- SEC505 Virginia Real Property Electronic Recording Standard
- SEC514 Removal of Commonwealth Data from Electronic Media Standard
- SEC525 Hosted Environment Information Security Standard
- Secure Remote Access to Online Court Documents Standard (SEC503-02.2)
- Security Awareness Training Standard (SEC527-00)

SDU-57 Suppliers of COV MDM services shall provide secure access to VITA or customer network via an MDM browser.

SDU-58 Any smart device that has installed a custom-built agency app or a COV-approved app from an app store shall have MAM software installed.

SDU-59 Suppliers of COV smart device services shall automatically quarantine a mobile device if malicious activity is detected or if directed by VITA or VITA customers.

SDU-60 Suppliers of COV smart device services shall provide device threat detection, remediation, and notification for the mobile devices in use by VITA and its customers.

SDU-61 Suppliers of COV smart devices shall provide on-device remediation actions such as disabling Wi-Fi, blocking application downloads, and blocking SMS/text messages.

SDU-62 Suppliers of COV smart devices shall provide VPN connectivity.

SDU-63 Suppliers of COV smart devices shall provide a smart device admin app that supports the following functions:

- Single-sign-on (SSO) across applications
- SAML, OAuth, Open ID Connect, and SCIM provisioning
- Password strength requirements
- 2-step verification and user managed security keys
- Domain-wide admin managed security keys
- Enforce security key usage to access services

SDU-64 Any BYOD smart device used to conduct official business and store commonwealth data shall apply partitions or containers to separate commonwealth data from personal data.

SDU-65 Any smart device at a minimum shall be configured with the approved security baseline configuration.