



## PURPOSE

The purpose of this policy is to create a prescriptive set of processes and procedures, aligned with applicable COV IT security policy and standard, to ensure the Virginia Information Technologies Agency (VITA) develops, disseminates, and updates the Mobile Device Access Controls Policy. This policy and procedure establishes the minimum requirements for mobile device access controls.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.1 Security Access Control Family, Control AC-19, to include specific requirements for the Commonwealth of Virginia.

## SCOPE

All VITA employees (classified, hourly, or business partners) who require access to VITA's IT systems

## ACRONYMS

CIO:	Chief Information Officer
ISO:	Information Security Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC501:	Information Security Standard 501
VCCC:	VITA Customer Care Center
VITA:	Virginia Information Technologies Agency

## DEFINITIONS

[See COV ITRM Glossary](#)

## BACKGROUND

Mobile access exposes the COV to substantial risk and vulnerability. As such proper controls are required to ensure that VITA owned and operated systems are protected and that risk is mitigated to the greatest extent possible. This policy directs that VITA meet the requirements as stipulated by COV ITRM Security Standard SEC501 and security best practices.

## ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Process section. The following Roles and Responsibility Matrix describe 4 activities:

- 1) Responsible (R) – Person working on activity

- 2) Accountable (A) – Person with decision authority and one who delegates the work
- 3) Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- 4) Informed (I) – Person who needs to know of decision or action

Roles	User	User Manager	System Owner	System Admin	Information Security Officer	Agency Head
<b>Tasks</b>						
USAGE RESTRICTIONS AND IMPLEMENTATION GUIDANCE FOR MOBILE DEVICES THAT ACCESS, PROCESS, OR STORE COV DATA					R	A
AUTHORIZES CONNECTION OF MOBILE DEVICES	I	C		R	A	
REGISTERS MOBILE DEVICE WITH AGENCY	I	C		R	A	
MONITORS FOR UNAUTHORIZED CONNECTIONS			A	R	I	
ENFORCING REQUIREMENTS FOR THE CONNECTION OF MOBILE DEVICES				R	A	
DISABLE INFORMATION SYSTEM FUNCTIONALITY THAT PROVIDES THE CAPABILITY FOR AUTOMATIC EXECUTION OF CODE ON MOBILE DEVICES			A	R	I	
APPLY ORGANIZATION-DEFINED QUARANTINE, INSPECTION AND PREVENTATIVE MEASURES TO MOBILE DEVICES				R	A	
READS/SIGNS ACCEPTABLE USE POLICY AND USES REASONABLE CARE IN PROTECTING MOBILE ASSETS	R	A				
ISSUE SPECIALLY CONFIGURED MOBILE DEVICES TO INDIVIDUALS TRAVELING TO LOCATIONS DEEMED TO BE A SIGNIFICANT RISK	I	C	A	R	I	
USE OF EXTERNAL INFORMATION SYSTEMS					A	

## STATEMENT OF POLICY

This statement of policy covers, SEC501, AC-19 Mobile Device Access Controls, AC-20 Use of External Information Systems, as well as, all related COV additions to those controls. This policy establishes the minimum requirements for the use of a COV owned and maintained mobile device, a non-COV owned and maintained mobile device, as well as any mobile device taken outside the borders of the COV that is used to access, process or store COV data. Enforcement of the restrictions outlined in this policy is accomplished by controls as implemented:

- VITA Logical Access Control Policy
- VITA IT Security Audit, Logging and Monitoring Policy
- VITA Security Awareness and Training Policy

## **A. ACCESS CONTROL FOR MOBILE DEVICES**

Mobile devices include cellular telephones, tablets and portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., personal digital assistants, digital cameras, and audio recording devices).

Organization-controlled mobile devices include those devices for which the agency has the authority to specify and the ability to enforce specific security requirements.

1. The Agency Head (or designee) shall establish usage restrictions and implementation guidance for VITA-controlled mobile devices.
  - a. The mobile device must be authorized by the Agency Head (or designee).
  - b. The mobile device must be registered with the ISO.
  - c. The mobile device must be marked in a manner to clearly identify the device as COV property and indicate a method of return if the device is lost.
  - d. The mobile device user must read and sign the Agency Acceptable Use Policy.
2. The ISO authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.
  - a. The mobile device must be configured to use an encrypted network connection at all times when accessing COV data.
  - b. The mobile device user must not connect non-COV devices to the COV mobile device. Wall and vehicle charging devices and devices that provide sound input and output are permitted.
  - c. The mobile device must backup all COV data at least once every 21 days to an approved COV device or service.
  - d. The mobile device must not be attached to a non-COV computing system without the written permission of the Agency Head or his/her designee.
  - e. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.
  - f. The mobile device must only utilize software developed by the Agency, a software vendor under contract to the Agency, or acquired via the device vendor's or suppliers' authorized application store.

- g. The mobile device must be configured to not allow the user to escalate the base privilege level.
  - h. The mobile device user must not tamper with security controls configured on the device.
  - i. The mobile device user must not install personal software on the mobile device.
  - j. The mobile device must install all security updates within 30-days of release by the original equipment manufacturer or the authorized device reseller.
  - k. The mobile device shall only store sensitive COV data if approved by the Agency Head or his/her designee.
  - l. The mobile device must be configured to require all sensitive COV data be encrypted.
  - m. The mobile device must utilize an industry-standard encryption protocol to store sensitive COV data (128-bit Advanced Encryption Standard at a minimum).
  - n. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.
  - o. The lost or stolen mobile device will be wiped within 24-hours of the incident. The wiping action will be initiated by a VCCC ticket.
  - p. If the mobile device is lost or stolen, the incident must be reported to the VITA Customer Care Center and Commonwealth Security and Risk Management Incident Management within 24-hours in accordance with §2.2-603(F) of the Code of Virginia.
  - q. Any mobile device to be decommissioned or transferred to another employee must adhere to the COV ITRM Removal of Commonwealth Data from Electronic Media Standard SEC 514.
  - r. The mobile device must be configured to store all COV data only on internal memory or non-removable media.
3. The ISO monitors for unauthorized connections of mobile devices to organizational information systems.
4. The ISO is responsible for enforcing requirements for the connection of mobile devices to organizational information systems.
- a. The mobile device must be configured to receive security policy and configuration information from the COV Mobile Policy Servers.
  - b. The mobile device screen lock must be configured to engage after a maximum of 15 minutes of inactivity.
  - c. The mobile device must be configured to prohibit the storage of passwords in clear text.

- d. The mobile device must be configured to automatically wipe the contents of the mobile device if 10 consecutive invalid login attempts occur.
  - e. Mobile device hardware options (wireless, infrared, Bluetooth, camera, GPS, etc.) that are not required for COV business functions (as defined by the Agency Head) must be disabled.
  - f. Mobile device applications that are not required for COV business functions (as defined by the Agency Head) must be disabled.
  - g. The mobile device must be configured to use a strong, complex password in accordance with the COV ITRM Information Security Standard.
  - h. The mobile device password must be changed after a period of 90 days.
  - i. The mobile device must be configured to not reuse a password prior to 24 password changes.
  - j. The mobile device must be configured not to cache/store passwords on the device.
  - k. The mobile device must be configured to suppress the display of passwords on the screen as the password is entered into the device.
5. The System Owner will disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.
  6. VITA will issue specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
  7. The System Administrator applies organization-defined quarantine, inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
  8. Users of mobile devices should use reasonable care in protecting mobile assets.
    - a. The physical security of the mobile device is the responsibility of the employee to whom the device has been assigned.
    - b. The mobile device must be protected at all times from unauthorized access.
    - c. The mobile device must not be left unattended in any area accessible by the general public.
  9. Users of non-COV owned mobile devices must follow these additional requirements:
    - a. The device must only be used to access COV data via the COV Messaging Service, a web service accessible from the public Internet, or from a COV internal network in accordance with the COV ITRM IT Standard Use of Non-Commonwealth Computing Devices to Telework SEC 511. This requirement does not apply to the use of Outlook Web Access or restrict the use of the device for

personal activities so long as those activities do not violate any other requirement of any existing COV policy.

- b. The mobile device user must agree in writing to allow remote wiping and the erasure of all COV data on the device without warning, if so requested by the Agency Head or the Agency Head designee. The mobile device user must agree in writing to allow remote wiping and the erasure of all data on the device without warning if the COV data cannot be removed without wiping the entire device.
- c. The mobile device user must agree to surrender the device to Commonwealth Security for review and forensic imaging upon request of the associated Agency Head or the Agency's Information Security Officer.

## **B. USE OF EXTERNAL INFORMATION SYSTEMS**

Note: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

1. The ISO shall permit authorized individuals to use an external information system to access the information system or to process, store, or transmit VITA-controlled information only when:
  - a. The ISO can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
  - b. The ISO has approved information system connection or processing agreements with the organizational entity hosting the external information system.
2. VITA employees and business partners who remotely access agency network resources will use only VITA-provided equipment configured, set up and maintained by VITA without modification.
3. Access to network resources, including the Internet, will be via broadband or modem dial-in and Virtual Private Networking (VPN). This does not apply to users accessing Microsoft Outlook Web Access from a remote location.
4. The ISO shall limit the use of organization-controlled portable storage media by authorized individuals on external information systems.
5. Users are not allowed to use or store personal IT assets in facilities that house IT systems and data.

## **ASSOCIATED PROCEDURE**

VITA Information Security Program Policy

## **AUTHORITY**

Page 6 of 7

Issuing Office: *Commonwealth Security & Risk Management*

File Name: VITA CSRM Mobile Device Access Controls v1\_0

Revised: 02/03/2014, v1.0

Superseded:

**REFERENCE**

[Code of Virginia, §2.2-2005 et seq.](#)

(Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency; "VITA")

**OTHER**

**REFERENCE**

[ITRM Information Security Policy \(SEC519\)](#)

[ITRM Information Security Standard \(SEC501\)](#)

Version History		
Version	Date	Change Summary
1	07/01/2014	Original. VITA CSRM Non-COV Mobile Device Security Policy, VITA CSRM COV Mobile Device Security Policy, and VITA CSRM Operation Travel Security Policy were updated and combined to form this new policy.