



COV Mobile Device Security Policy

EFFECTIVE DATE: 11/09/2011, v1

Only the VITAweb Portal has the current version. Verify copy against VITAweb.

PURPOSE: To document the Virginia Information Technologies Agency (VITA) policy on the use of Commonwealth of Virginia (COV) owned mobile computing devices to access to COV information technology (IT) resources in conjunction with the COV Information Technology Resource Management (ITRM) IT Security Policy SEC519-00.

SCOPE: All VITA employees, business partners, and those that contract with VITA for services.

ACRONYMS:

BIA:	Business Impact Analysis
CSRM:	Commonwealth Security and Risk Management
COV:	Commonwealth of Virginia
IM:	Incident Management
ISO	(VITA) Information Security Officer
IT:	Information Technology
VITA:	Virginia Information Technologies Agency

DEFINITIONS: See [COV ITRM Glossary](#)

STATEMENT OF POLICY/POLICY:

This Policy establishes the minimum requirements for the use of a COV owned and maintained mobile device to access, process, or store COV data in accordance with [IT Security Standard \(SEC501\)](#). This Policy stipulates the enhanced controls required for mobile devices and does not rescind the obligation to adhere to COV ITRM SEC501-06. At a minimum the selection, implementation and use of mobile devices include the following elements:

Prior to Use

1. The mobile device must be authorized by the Agency Head or his/her designee.
2. The mobile device must be registered with the Agency's Information Security Officer.
3. 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.
4. The mobile device user must read and sign the Agency acceptable use policy.

Configuration Requirements

1. The mobile device must be configured to receive security policy and configuration information from the COV Mobile Policy Servers.
2. The mobile device screen lock must be configured to engage after a maximum of 15 minutes of inactivity.

3. The mobile device must be configured to prohibit the storage of passwords in clear text.
4. The mobile device must be configured to automatically wipe the contents of the mobile device if 10 consecutive invalid login attempts occur.
5. 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.
6. Mobile device applications that are not required for COV business functions (as defined by the Agency Head) must be disabled.

Password Requirements

1. The mobile device must be configured to use a strong, complex password in accordance with the COV ITRM Information Security Standard.
2. The mobile device password must be changed after a period of 90 days.
3. The mobile device must be configured to not reuse a password prior to 24 password changes.
4. The mobile device must be configured not to cache/store passwords on the device.
5. The mobile device must be configured to suppress the display of passwords on the screen as the password is entered into the device.

Connectivity Requirements

1. The mobile device must be configured to use an encrypted network connection at all times when accessing COV data.
2. 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.
3. The mobile device must be connected to an approved/assigned COV software sync station to backup all COV data at least once every 21-days.
4. 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.

Software Requirements

1. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.
2. 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.
3. The mobile device must be configured to not allow the user to escalate the base privilege level.
4. The mobile device user must not tamper with security controls configured on the device.
5. The mobile device user must not install personal software on the mobile device.
6. The mobile device must install all security updates within 30-days of release by the original equipment manufacturer or the authorized device reseller.

Data Storage Requirements

1. The mobile device shall only store sensitive COV data if approved by the Agency Head or his/her designee.
2. The mobile device must be configured to require all sensitive COV data be encrypted.
3. The mobile device must utilize an industry-standard encryption protocol to store sensitive COV data (128-bit Advanced Encryption Standard at a minimum).
4. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.
5. The mobile device must be configured to store all COV data only on internal memory or non-removable media.

Physical Security Requirements

1. The physical security of the mobile device is the responsibility of the employee to whom the device has been assigned.
2. The mobile device must be protected at all times from unauthorized access.
3. The mobile device must not be left unattended in any area accessible by the general public.
4. 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.
5. 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.
6. 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.

ASSOCIATED
POLICY/
PROCEDURE: None

AUTHORITY
REFERENCE: [Code of Virginia, §2.2-2005, et seq.](#)
(Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency; "VITA")

[Code of Virginia, §2.2-2827](#)
(Restrictions on state employee access to information infrastructure)

[COV Information Security Policy, ITRM Policy SEC519-00](#)

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

[Code of Virginia, §2.2-603\(f\)](#)
(Authority of agency directors)

OTHER

REFERENCE: [Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard \(SEC514\)](#)

[IT Risk Management Guideline](#) (SEC506)

[IT Data Protection Guideline](#) (SEC507)

[IT Systems Asset Management Guideline](#) (SEC518)

Commonwealth Policies, Standards, and Guidelines (PSG):
<http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs>

VITA Internal Policy Website:
<https://vashare.virginia.gov/sites/vita/Resources/PP/Pages/Default.aspx>

National Institute of Standards and Technology FIPS 140-2
<http://csrc.nist.gov/groups/STM/cmvp/standards.html>

Version History		
Version	Date	Change Summary
1	11/09/2011	Original document, which aligns VITA with the requirements in the <i>IT Security Standard</i> (SEC501-06)