Policy and Procedure

Virginia Department of Agriculture and Consumer Services

Number 10.6

SUBJECT: Mobile Device Security Policy (COV-owned Devices)

Date: July 25, 2014
Revision: July 25, 2014
Effective: August 1, 2014

APPROVAL: Sandra J. Adams

OBJECTIVE AND INTENT

The Virginia Department of Agriculture and Consumer Services (VDACS) provides the Commonwealth of Virginia (COV) owned mobile computing devices to access COV information technology resources to employees approved for such devices. The COV owned mobile devices are additionally governed by agency policy 10.1, *Ethical Use of Agency Information and Computing Resources* and COV Security Standard, SEC501.

SCOPE

All VDACS employees and its agents, including all classified, wage, seasonal, temporary agency and contract personnel who have been approved for the use of a COV owned mobile computing device must comply with this policy and any additional policies that may be adopted relating to mobile device technology.

STATEMENT OF 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 Security Standard SEC501.

A. ACCESS CONTROL FOR MOBILE DEVICES

1. Prior to use.

    a. The mobile device must be authorized by the Agency Head (or designee).

    b. The mobile device must be registered by the Agency Telecommunications Coordinator with the Agency's 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 VDACS Policy 10.1, *Ethical Use of Agency Information and Computing Resources*.

    e. The mobile device user must have read and signed Attachment A, *Acknowledgement of Acceptable Use of COV Owned Mobile Device.*

2. Configuration Requirements.

    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.

3. Password Requirements.

   a. The mobile device must be configured to use a password in accordance with the COV ITRM Information Security Standard (minimum of 4 characters for a mobile device).

   b. The mobile device password must be changed after a period of 90 days.

   c. The mobile device must be configured to not reuse a password prior to 24 password changes.

   d. The mobile device must be configured not to cache/store passwords on the device.

   e. The mobile device must be configured to suppress the display of passwords on the screen as the password is entered into the device.

4. Connectivity Requirements

   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 be connected to an approved/assigned COV software sync station to backup all COV data at least once every 21 days.

   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.

5. Software Requirements

   a. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.

   b. 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.

   c. The mobile device must be configured to not allow the user to escalate the base privilege level.

   d. The mobile device user must not tamper with security controls configured on this device.

   e. The mobile device must install all security updates within 30 days of release by the original equipment manufacturer or the authorized device reseller.

6. Data Storage Requirements

   a. The mobile device shall only store sensitive COV data if approved by the Agency Head or his/her designee.

   b. The mobile device must be configured to require all sensitive COV data be encrypted.

   c. The mobile device must utilize an industry standard encryption protocol to store sensitive COV data (128-bit Advanced Encryption Standard at a minimum).

   d. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.

   e. The mobile device must be configured to store all COV data only on internal memory or non-removable media.

7. Physical Security Requirements

   a. Each employee authorized to use a mobile communications device to conduct the business of the Commonwealth is responsible for the reasonable care and due diligence in using, handling and protecting the mobile device.

   b. Every employee shall take reasonable precautions to protect mobile communications devices assigned to them from damage, loss, theft, fraud or other misuse.

   c. Mobile devices shall not be left in unattended personal or state vehicles. The only exception to this is if an employee is required to enter a government or courts building which will not allow mobile devices. In that instance, the mobile device should be locked in the trunk of a vehicle but care should be taken to ensure no one observes the device being left in the car.

   d. 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.

   e. If the mobile device is lost or stolen, the incident must be reported to the employee's supervisor, the VDACS ISO, 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.

   f. 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.

8. Safe and Courteous Operations

   a. Mobile communication devices shall not be used while driving, except in cases of emergency, during which times they may only be used for voice communications.
   b. They may be used with a hands free device in limited situations, but not for prolonged conversations or in heavy and/or slow moving traffic.
   c. Text messaging while driving is strictly prohibited under all circumstances.
   d. Many states and the District of Columbia have enacted laws that prohibit the operation of a motor vehicle on a public highway while using a wireless telephone. Be familiar with and abide by state laws regarding wireless phone use.

9. International Travel

   a. All assigned COV electronics must remain within the Continental USA
   b. Travel outside the Continental USA requires the use of temporary devices that contain the absolute minimum data to accomplish the purpose of the trip.
   c. Immediately upon return from an international trip:

i. ... Do not connect any device to a COV network until that device has been examined and cleared by the agency IT staff.

ii.... Immediately return the device(s) to the agency Telecommunications Coordinator who will direct a member of the IT staff to examine the devices(s) for the presence of malicious software. Do not connect the device to the COV network. (This may require disabling of the network connection setting in your device.)

iii... Change all system and account passwords using a system within the agency network.

iv... If the computing asset was used outside the Continental USA, the asset must be completely erased in accordance with the COV ITRM SEC 514 Data Removal Standard. The IT Director will request such erasure by submitting a VCCC ticket.

B. NO EXPECTATION OF PRIVACY

1. Except where prohibited by law, employees do not have, and shall not expect, privacy while using any Commonwealth owned mobile communications device. This includes usage detail information, telephone numbers dialed and received, data transmission content, and email. Additionally, the Commonwealth reserves the right to use Global Positioning System (GPS) or other location tracking functionality on all Commonwealth owned devices.

C. INCIDENTAL PERSONAL USE

1. Incidental personal use of the Commonwealth owned device is permitted as long as it does not materially or routinely impact the cost of service to the Commonwealth.

AUTHORITY

The Commissioner of Agriculture and Consumer Services issues this policy pursuant to authority granted under the laws and regulations of the Commonwealth of Virginia.

INTERPRETATION

The Director of Administrative and Financial Services is responsible for official interpretation of this policy.

ATTACHMENTS

A - Acknowledgement of Acceptable Use of COV Mobile Device Security Policy
B - Use of Mobile Devices While Traveling Domestically and Internationally
C - Telecommunications Work Order
D - Using COV Mobile Devices to Conduct VDACS Business

ATTACHMENT A
Virginia Department of Agriculture and Consumer Services

Acknowledgement of Acceptable Use of COV Mobile Device Security Policy

I understand and agree to abide by current and subsequent revisions to the VDACS Policy for COV Mobile Device Policy and the Code of Virginia, Section 2.2-2827.

I understand that VDACS has the right to monitor any and all aspects of the COV Mobile Device related to Commonwealth of Virginia data and that this information is a matter of public record and subject to inspection by the public and VITA management for all mobile devices used in the interest of the Commonwealth. I further understand that users should have no expectation of privacy regarding any usage as it relates to Commonwealth of Virginia data. I also understand and agree to produce any public record required by the agency, if requested. By signing this use agreement I agree 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. Furthermore, I agree to allow remote wiping and the erasure of all data on the mobile device if the COV data cannot be removed from the device without removing all data from the device. I also 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.

I further understand that misuse and/or negligent use of a mobile device may result in disciplinary action (up to and including dismissal) and forfeiture of my privilege to use mobile devices. I further understand that the Human Resource Office may access the VDACS Knowledge Center to verify that I have read this policy. Employees will be required to review this policy whenever the mobile device policy is updated. I further understand that I may download a copy of this policy with all three Appendices from the VDACS Intranet.

By responding "True" to the Policy Acknowledgement on the VDACS KC you are certifying that you have read and/or participated in this training activity to the fullest extent possible.

1. Upon completion of the policy review, exit the course. You are taken to the Course Detail Screen.

2. Wait for the Course Detail Screen to update, verifying that you have completed the course.

3. From the updated Course Detail Screen, click "View Certificate". When the Certificate of Completion displays, click print. Submit the certificate with the Telecommunications Work Order through your supervisor and division director to the Telecommunications Coordinator

ATTACHMENT B
Virginia Department of Agriculture and Consumer Services

Use of Mobile Devices While Traveling Domestically and Internationally

It is the policy of the Commonwealth of Virginia to ensure the confidentiality, integrity, and availability of data provided to and generated by all Commonwealth agencies. Trustworthy data, whether classified as sensitive or non-sensitive, is critical to daily agency operations. Please keep the following in mind when traveling with an agency computing device.

Preparing for the Trip

- Review the information required for the trip. Do not take information that is not needed to accomplish the purpose of the trip, including sensitive contact information.
- Consider the consequences if the information were to be stolen by a foreign government or a malicious individual. If the device is lost, stolen, or otherwise compromised, the sensitive data could also be compromised.
- Private data that is required for the trip, but cannot be stored on a computer, must be copied onto an encrypted USB memory device.
- Please note that in some countries, customs officials may not permit you to enter with encrypted information. Research such restrictions prior to departure and contact the appropriate federal agency (U.S. Department of State, etc.) to file any necessary requests for exemption, if available.
- Use encryption with complex passwords to protect confidential files.
- Back up all information required for the trip and secure the backed-up data at the office.
- If operationally feasible, acquire temporary computer assets for use during the trip.
- Travel outside the Continental USA requires the use of temporary devices that contain the absolute minimum data to accomplish the purpose of the trip.
- Change the password for any account to be used during the trip.
- Never store passwords, phone numbers, or sign-on sequences on any device or its case.

Preparing the Computing Asset

- Have Information Systems change the administrator account password.
- Install all operating system updates.
- Install all anti-virus, firewall, and anti-spyware security application software updates.
- Encrypt the computer hard disk or at least all sensitive information on the device.
- Update the web browser software and implement strict security settings.
- Update all application software to be used during the trip.
- Disable infrared ports, Bluetooth ports, web cameras, and any hardware features not needed for the trip.
- Configure the device to use a VPN connection to create a more secure connection.
- Configure the device to disable sharing of all file and print services.
- Configure the device to disable ad-hoc wireless connections.

General Travel Precautions

- Avoid using computer bags to carry the laptop since it is obvious that the bag contains a laptop.
- Transport the laptop in a padded briefcase, suitcase, or backpack that can be locked in a discrete manner.
- Avoid transporting devices in checked luggage.
- Change passwords at least every 4 days for all electronic devices and remotely accessed accounts.
- Use digital signature and encryption capabilities when possible.

- Do not leave electronic devices unattended.
- If you have to leave the device, or the device will not be used for an extended period, remove the battery, any memory or SIM cards and keep them with you.
- Do not use thumb drives given to you as the thumb drive may be compromised or contain malicious software.
- Assume that any computer not provided by COV is not secure and may be compromised with malicious software. This includes public terminals found in libraries and cyber cafes.
- If a shared system must be used, do not enter sensitive information such as passwords, bank account numbers, or credit card numbers since any sensitive data sent over the internet from a public access point may be intercepted and logged by unknown parties.
- Do not use the "remember me" feature on websites. Re-enter the password for the website every time.
- Terminate connections when not in use.
- Clear the browser session data after each use: delete history files, caches, cookies, URL, and temporary internet files.
- Do not open emails or attachments from any source without verifying the legitimacy of the source and the contents of the message.
- Do not click on links in emails.
- Empty the "trash" and "recent" folders after every system use.

Hotel and Airport Considerations

- Do not leave your computing device at the front desk. It is not the responsibility of the hotel to protect a guest's property.
- If the device must be left in the hotel room, place it in the hotel room safe if available. If the room does not have a safe, secure the device to a piece of furniture with a security cable.
- If traveling by car, keep all devices out of sight by locking the device in the trunk. Keep in mind, however, that if temperatures are extreme, your device battery could suffer and your hard drive could be destroyed.
- If traveling by air or rail, hold the bag containing all devices until the person in front of you has gone through the screening process.
- Avoid setting the bag containing the devices on the floor since this is an easy way to forget or lose track of the bag.

Traveling Outside the Continental USA

- All assigned COV electronics must remain within the Continental USA
- Travel outside the Continental USA requires the use of temporary devices that contain the absolute minimum data to accomplish the purpose of the trip.
- Be aware that government security agencies in some countries may log all internet activity without prior notification.
- Be aware that in some countries it is common practice for the government or businesses to copy data from any computer system without the user's knowledge or consent.
- Be aware that all personal belongings may be searched multiple times and electronic media may be copied.
- Many countries do not grant any expectation of privacy in internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries and hotel rooms are often searched.
- Do not transfer sensitive information onto a computer that has left the Continental USA.
- Do not attach any removal media such as a thumb drive or memory card to a foreign computer. The system may contain malicious software and should be considered compromised.

- Foreign security services and criminals can track your movement using the hardware inside your computing asset and can enable hardware such as the web camera or microphone without any warning. To prevent this, remove the battery if possible, and disable the camera and microphone capabilities on all electronic devices when those functions are not being used.
- Foreign security services and criminals can also insert malicious software into your device through any connection they control including any wireless connection enable on the device.
- If a customs official demands to examine the computing asset, or if the hotel room is searched while the computing asset is unattended, assume the asset's hard drive has been copied.
- Be cautious of unsolicited requests and questions about the purpose of the trip or other sensitive information.
- It is advisable to not speak about the purpose of the trip or comment on the status of the trip.
- Avoid political conversations or offering political opinions while in foreign countries, either in person, on the phone, or online.
- Avoid wireless networks if possible. In some countries the wireless networks are controlled by state security services; in all cases, the networks are not secure.
- Assume anything on your computer will be read by someone.
- Assume your device will be lost or stolen.

Upon Returning from the Trip

- Do not connect any device to a COV network until that device has been examined and cleared by the agency IT staff.
- Immediately return the device(s) to the agency Telecommunications Coordinator who will direct a member of the IT staff to examine the devices(s) for the presence of malicious software. Do not connect the device to the COV network. (This may require disabling of the network connection setting in your device.)
- Change all system and account passwords using a system within the agency network.
- If the computing asset was used outside the Continental USA, the asset must be completely erased in accordance with the COV ITRM SEC 514 Data Removal Standard. The IT Director will request such erasure by submitting a VCCC ticket.

Incident Handling or Loss of Device

- If your device is lost or stolen, change all account passwords from a secure computing asset to prevent unauthorized access to COV servers.
- If a secure computing asset is not available, contact the agency IT director to have all affected accounts disabled until your trip ends.
- If the device is lost or stolen, the incident must be reported to your supervisor, the VDACS ISO, 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.
- If traveling outside the Continental USA, report the theft of the device or information to your supervisor, the VDACS ISO, 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. You should also report the loss/theft to the local US embassy or consulate.

Final Thoughts

- It is not a question of **IF** the system will be compromised, but **WHEN** will the system be compromised.
- Do not take the device unless it is really, really needed.
- Carefully consider the benefits of traveling with computing assets versus the costs of a successful compromise of your sensitive data.
- Use temporary devices for all travel and wipe the device both before and after travel.
- Disable all communication ports including Bluetooth, Wi-Fi, cameras, and microphones on all devices.
- If the device is not being used, remove the battery to prevent malicious software from enabling communication ports.
- Connect to the internet only through an encrypted, password-protected channel.
- Many countries prohibit travelers from entering the country with encrypted devices unless they have government permission.

ATTACHMENT C
Virginia Department of Agriculture and Consumer Services

VDACS TELECOMMUNICATIONS WORK ORDER (TWO)

Note: Items highlighted in yellow are required fields.

Request Type

□ Add　　□ Move/Change　　□ Disconnect/Delete

Service Needed

□ Analog Line
□ Air Card
□ Cell Phone
□ iGear
□ Mobile Device (iPad/iPhone)
□ VoIP Phone Service
□ "Secure Mail App"
□ Other
□

Date: ____________　　Name of State Purchase Card User to be charged: ____________

Requestor's Name: ____________　　Alternate Contact Name: ____________

Phone Number: ____________　　Cost Code: ____________

Date Service to begin: ____________　　Division: ____________

Employee Name Last name, First Name	Device Brand/Model/Type	Is a New Number needed? Yes/No	Address, City, State, Zip Code Home address or VDACS Facility

Good Technology – Software installed on the mobile device that allows for secure email (cost is $143.49 per license plus $15.22 per month for each device)

Employee Name	COV Email Address	Device Model	Device phone number

Additional Information: Attach additional sheets if needed

Approvals

Supervisor's Signature:　　Date:

Division Director's Signature (required for smart phones and mobile devices):　　Date:

If you are having functionality problems with your equipment call 804/786-4724 or email Jake.jacobs@vdacs.virginia.gov
http://barley.vdacs.state.va.us:7778/intranet/telecommunications_work_order.doc

ATTACHMENT D
Virginia Department of Agriculture and Consumer Services

USING COV MOBILE DEVICES TO CONDUCT VDACS BUSINESS

Employees may request a COV smart phone (iPhones only) or iPad to conduct agency business. The process for requesting and obtaining approval is explained below.

TASK #	TASK	RESPONSIBLE PERSON	ADDITIONAL INFORMATION
1	Review COV Mobile Device Security Policy on the Commonwealth of Virginia Knowledge Center (KC), VDACS Domain at https://covkc.virginia.gov/vdacs. (Policy 10.6)	Employee	1. The policy review must be marked complete to acknowledge reading, understanding and accepting the policy. 2. Save the web acknowledgement page in a PDF format so that employee name and the date marked as complete in the KC is visible and submit with your request. 3. The order will NOT be processed without the policy marked complete acknowledgement
2	Complete a VDACS Telecommunications Work Order Form at on InSite at http://barley.vdacs.state.va.us:7778/intranet/facilities.htm and submit to your supervisor along with the 10.6 policy acknowledgement.	Employee	
3	Review and approve Telecommunication Work Order Form. Ensure KC policy acknowledgement is attached. Submit the approved Telecommunication Work Order form to the VDACS Telecommunications Coordinator, jake.jacobs@vdacs.virginia.gov	Supervisor	
4	Complete a Telecommunications Service Request (TSR) for device and cell/data service.	Telco Coordinator	Once the hardware is received, forward a copy of the VDACS Telecommunications Work Order to Information Systems Support.
5	Complete a TSR and submit to VITA for the Enterprise Handheld Service (EHS)	Telco Coordinator	
6	Monthly, verify that proper cost codes are billed for the EHS services.	Telco Coordinator and IS Support	The Good Licenses will be charged on the VITA Comprehensive invoice and the Airwatch licenses will be charged to the VITA Telecommunications invoice.
7	Track COV mobile devices and Good licenses. Record in EHS inventory. Post the inventory to ensure that the ISO has access to the information.	Telco Coordinator	Inventory information is posted on the network at J:\Telecommunications
8	Request a monthly report from VITA/NG of mobile devices that have checked in with the EHS server. Review to identify any unused EHS Licenses.	IS Support	Confirm with VITA that agency will be notified when the EHS application is no longer being used by staff. VITA will not commit to a monthly report on these services but the IT staff can request the list each month.

Notes:

1. HRO - Employee policy acknowledgements will be maintained through the COV KC/VDACS domain.
2. Employee – VITA/NG automatically pushes the EHS application to the mobile device.
3. Employee - Register with iTunes and/or iCloud using their personal credit card
4. Employee – Download personal apps on personal device and on COV device using personal credit card
5. Employee – If a business application is needed, request approval from program manager, division director and IT director via email before completing the download.
6. Employee – If there is a cost for a business application, attach emailed approvals to the employee reimbursement documentation and submit to the Finance Office for reimbursement through standard employee reimbursement process.
7. Telco Coordinator will purchase covers for the iPhones. The program area is responsible for the purchase of all accessories for all devices except for iPhone covers. **It is required that iPad covers be purchased to protect the device.**
8. The VCCC is responsible for support of EHS Technology.
9. The service provider is responsible for support of the device.