

<p style="text-align: center;">State of Rhode Island Department of Administration Office of Information Technology</p>	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

1. Background

Once viewed as “cool” gadgets for early adopters, Mobile Devices have become indispensable tools offering the State and its employees numerous advantages. However, the dramatic proliferation and increasing ability of Mobile Devices to store, process, and transmit data poses a significant threat to the security of State data and infrastructure. On average, more than 10,000 Mobile Devices are stolen every day throughout the United States - a dramatic increase over the past decade. The cost associated with the loss of a Mobile Device far outweighs the cost of the device itself, especially when sensitive data is compromised. Through the implementation of basic security controls, along with Users practicing some common sense measures, the State can significantly reduce risk associated with the use of Mobile Devices within the workplace environment.

2. Purpose

To provide policy and guidance for appropriately managing and securing Mobile Devices that store, process, and/or transmit State data in order to effectively reduce the risk associated with allowing the use of Mobile Devices within the workplace environment.

3. Scope

This policy covers all State Executive Branch Departments¹ (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State, via a Mobile Device.

4. Authority

R.I. Gen. Laws § 42-11-2.8 establishes the Division of Enterprise Technology Strategy and Services (“ETSS”) within the Department of Administration. Pursuant to R.I. Gen. Laws § 42-11-2.8(b)(1), the Office of Information Technology (“OIT”), under ETSS, “shall manage and support all day-to-day operations of the state’s technology infrastructure, telecommunications, and associated applications”.

5. Acronyms and Definitions

Apple App Store – Apple’s platform for the digital distribution of mobile applications that run on Apple’s iOS operating system. The Apple App Store allows users to browse, purchase, and download available applications via iPhones, iPads, iPods, Apple TV, and computers.

App Catalog – Managed applications that allow for administrative control over some aspects of application functionality. Applications in the App Catalog tend to be business related (e.g. Microsoft Office apps).

¹ State Executive Branch Departments do not include the University of Rhode Island, the State colleges, Lieutenant Governor, State Treasurer, the Attorney General and State Secretary of State.

<p style="text-align: center;">State of Rhode Island Department of Administration Office of Information Technology</p>	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

CISO – The Chief Information Security Officer within ETSS.

Chief Digital Officer – As established by R.I. Gen. Laws § 42-11-2.8(a), the individual appointed by the Director of Administration who oversees the ETSS.

DoIT – Refers to the Division of Information and Technology which shall now mean the ETSS in accordance with R.I. Gen. Laws § 42-11-2.8(a).

ETSS – The Division of Enterprise Technology Strategy and Services established by R.I. Gen. Laws § 42-11-2.8(a).

Managed App – Applications available for download via the App Catalog. All other applications are unmanaged apps (those not in the App Catalog but available for download via the Apple App Store).

Mobile Device – A computing device that is easily portable, has its own operating system, and is able to run application software. Typically, Mobile Devices have a display screen, a method to input data (e.g. touch screen, touch keyboard, miniature keyboard), and the ability to communicate and transfer data wirelessly (e.g. Wi-Fi, Bluetooth). Examples of Mobile Devices include, but are not limited to, tablets, laptops, notebooks, smartphones, and any other portable computing device.

Mobile Wallet Applications – Mobile Device applications that allow for the use of a Mobile Device to transfer funds or pay for in-store transactions at retail locations by linking the application to the user’s credit card, debit card, or bank account. Transactions are usually initiated and performed by using either NFC (Near Field Communications) protocols or QR (Quick Response) barcodes at point of sale terminals. Mobile wallet applications include, among others, Apple Pay (for iPhones), Android Pay (NFC-enabled Android devices), Samsung Pay (Samsung phones), Google Wallet (NFC-enabled iOS and Android devices), and Current C (iOS and Android phones).

OIT – The Office of Information Technology within the Division of Enterprise Technology Strategy and Services.

Supervised Device – Any State-owned Mobile Device running the Apple iOS operating system.

User - An individual who uses a personal or State owned Mobile Device to access State networks, applications, and/or data.

6. Policy

6.1. General Rule. As a general rule, only State owned Mobile Devices are authorized to access State data and network resources. Personally owned Mobile Devices are explicitly prohibited from storing, processing, or transmitting State data or connecting to State network resources unless prior authorization and formal approval has been granted.

6.2. User Agreement. Prior to using a Mobile Device for storing, processing, or transmitting State data or connecting to State network resources, Users must have a signed and formally approved

<p style="text-align: center;">State of Rhode Island Department of Administration Office of Information Technology</p>	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

Mobile Device Security Policy User Agreement form attached hereto as **Appendix A** on file. In addition, Users participating in the Bring Your Own Device Program must have a signed and formally approved *Bring Your Own Device Security Policy User Agreement* form on file (form located in Appendix A of DoIT Policy 10-27 entitled *Bring Your Own Device Security*). Existing users may be able to accept and digitally sign this policy in response to an Office of Information Technology email which would require a user to respond via electronic approval.

- 6.3. **Mobile Wallet Applications.** Mobile Wallet Applications will not be installed on any State owned Mobile Device. State credit cards will not be entered or associated with any Mobile Wallet Application installed on personally owned Mobile Devices.
- 6.4. **Network Authentication.** Users will authenticate to the State network with a unique User ID and password prior to being granted access. Any Mobile Device software that utilizes a script file to access State data and network resources will not contain the User ID or password within the script.
- 6.5. **Antivirus Software.** Mobile Devices will have up-to-date anti-virus software and the latest security patches installed. Security patches for high-risk vulnerabilities should be installed within two (2) days of the notification of availability. Mobile Devices will be scanned to ensure that up-to-date anti-virus software and the latest security patches are installed. Mobile Devices that do not meet the criteria will be denied access to the State network.
- 6.6. **Untrusted Networks.** Users should not connect to untrusted networks (i.e. any non-State network) because these networks are considered insecure and pose an increased risk of sensitive or confidential data being compromised. If absolutely necessary and there is no other alternative, Users connecting to any public or private non-State network (e.g. hotels, restaurants, airports, train stations, home), either wired or wirelessly, should: (i) enable the firewall on the Mobile Device; (ii) disable file sharing on the Mobile Device; and (iii) enable file encryption on the Mobile Device (always back up encryption certificates). If more than one wireless network is accessible, verify the name of the wireless network prior to connecting to it (e.g. ask hotel front desk for the name of its wireless network).
- 6.7. **Incident Reporting.** Mobile Device Users will notify their supervisor, the Service Desk, and/or the Chief Information Security Officer, as appropriate, immediately upon becoming aware of an actual or suspected loss, theft, or unauthorized access of a Mobile Device in order to report the incident. Incidents involving Mobile Devices will be handled in accordance with DoIT Policy 10-12 entitled *Incident Handling and Response*. Once every 24 months, the State will cover the replacement cost of the first occurrence in which a Mobile Device User breaks, loses, or has stolen, whether accidental or not, his/her Mobile Device. Upon the second and each subsequent occurrence during each 24-month period, the Mobile Device User will be responsible for covering the replacement cost of the Mobile Device. The 24-month period commences on the date that the Mobile Device is assigned to the User and expires 24 months from that date. Upon expiring, the 24 month period will automatically renew for a new term of 24 months for as long as the Mobile Device remains assigned to the User.

<p style="text-align: center;">State of Rhode Island Department of Administration Office of Information Technology</p>	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

- 6.8. Physical Security.** Mobile Devices will be physically secured at all times, regardless of whether or not the device is being used. Mobile Devices will not be left unattended within unsecured areas at any time (e.g. any non-State facility, any publicly accessible area, home). If this is not possible, physical access to the Mobile Device will be appropriately restricted (e.g. placed inside a locked cabinet, locked office, behind a locked door). Mobile Devices will not be left in view of or physically accessible to others when not being used. With regard to vehicles, if no other option is available, Mobile Devices may temporarily be placed out of view in the trunk of a vehicle. However, Mobile Devices will not, at any time, be left anywhere inside a vehicle overnight.
- 6.9. Security Cable.** If appropriate for the type of device (e.g. laptop), a locking security cable will also be provided at the time the Mobile Device is issued. Users provided with a locking security cable will physically secure the Mobile Device to an immovable object whenever the device is being used.
- 6.10. Passwords.** Mobile Devices will be password protected. Mobile Device passwords will be configured in accordance with DoIT Policy 10-01 entitled *Enterprise Password Security*. If unable to meet these requirements, Mobile Device passwords will be as strong as the device will allow. Mobile Device passwords will be encrypted on the device.
- 6.11. Software Installation.** Mobile Device Users will not install any software on the device without prior authorization.
- 6.12. Screen Lock.** Mobile Devices will have the password-protected screen locking feature (e.g. screensaver) enabled at all times. The screen lock feature will be set to automatically lock the Mobile Device after no more than ten (10) minutes of inactivity.
- 6.13. Wireless Ports.** Mobile Device wireless ports will be disabled when not in use and Bluetooth will be set to "non-discoverable" mode.
- 6.14. Data.** All sensitive or confidential data stored on Mobile Devices will be encrypted. Data will be classified in accordance with DoIT Policy 05-02 entitled *Data Categorization* and encrypted in accordance with DoIT Policy 05-03 entitled *Data Encryption*. Users should use good judgment and limit the amount of sensitive or confidential data stored on Mobile Devices to only what is absolutely necessary in order to minimize the risk of compromising sensitive or confidential data from a lost or stolen device. The entire drive (e.g. hard disk drive, solid state drive) of Mobile Devices containing sensitive or confidential data will be encrypted in accordance with DoIT Policy 05-03 entitled *Data Encryption*. Mobile Device Users will not disclose any data that is stored on or accessible via Mobile Devices to unauthorized individuals. Data stored on Mobile Devices will be periodically backed up.
- 6.15. Supervised Device Security.**
- 6.15.1.** OIT will manage and maintain authority over all Supervised Devices. OIT may disable or remotely wipe Supervised Devices at any time in the event of an emergency, an actual or suspected security incident, a loss or theft of the device, or for any other reason.

<p style="text-align: center;">State of Rhode Island Department of Administration Office of Information Technology</p>	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

- 6.15.2. The only applications officially approved by OIT to be installed on Supervised Devices are the managed apps available in the App Catalog. All other applications (those available via the Apple App Store) are unmanaged applications and, therefore, not approved for install. Users should only install unmanaged applications if there is justification for valid business use. OIT will perform a quarterly review of installed applications on all Supervised Devices and notify Agency directors, as appropriate, to ensure valid business use and compliance with DoIT Policy 00-02 entitled *Acceptable Use*.
- 6.15.3. Users will not use personal email accounts to conduct State business and will not forward emails or email attachments from State email accounts to personal email accounts. Users will not use unmanaged apps to open files, documents, or attachments that can be opened by managed apps.
- 6.15.4. Applications often require permission to access specific functions on Supervised Devices in order to enhance the user experience and provide functionality. However, some privileges allow applications to access personally identifiable information and other sensitive data. Users will thoroughly review all permissions prior to installing any unmanaged application to ensure State data is not placed at undue risk of being compromised.
- 6.15.5. User accounts created to download applications from the Apple App Store to Supervised Devices will be set up using the State employee's email address. Passwords for this account will not be the same as any password used by the employee to access any State system or network.
- 6.15.6. Apple App Store applications purchased via a Supervised Device will not appear on the monthly State cell phone bill and can only be made via a personal credit card (not a State credit card) that is linked to the User account. In general, these purchases are the responsibility of the User and are not eligible for reimbursement. Unmanaged app purchases eligible for reimbursement by the State must be submitted to the Office of Accounts and Control via an expense report and allocated to the agency's RIFANS account.
- 6.15.7. Supervised Devices have limited memory. Users are responsible for ensuring that installed unmanaged apps do not adversely affect the operational integrity and performance of Supervised Devices. OIT will not provide support for any issue arising from the use of installed applications, including those in the App Catalog.
- 6.16. **Issuance.** This policy becomes effective upon approval and shall supersede all previously issued versions of this policy. The agency is responsible for disseminating and ensuring the review of this policy by all applicable individuals within the scope of this policy.
- 6.17. **Noncompliance.** Any employee who willfully violates this policy may be subject to disciplinary action up to and including termination of employment.

State of Rhode Island Department of Administration Office of Information Technology	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

6.18. Waivers. An agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the agency director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the Chief Information Officer. Waivers expire one year from date of issue, whereupon they must be renewed.

6.19. Amendment. This policy may be amended or rescinded at any time without further notice.

7. Roles and Responsibilities

Chief Information Security Officer

- Periodically review and update this policy.
- Assist the agency when a Mobile Device is lost or stolen, as required, and take appropriate actions when sensitive or confidential data is compromised.
- Perform a quarterly review of installed applications on all Supervised Devices and notify agency directors, as appropriate, to ensure valid business use and compliance with DoIT Policy 00-02 entitled *Acceptable Use*.

Agency

- Comply with all provisions documented in this policy.
- Require that all Users issued a Mobile Device sign the *Mobile Device Security Policy User Agreement* form in **Appendix A** of this policy and maintain the signed forms on file.
- Periodically account for all issued Mobile Devices.
- Allocate to the agency's RIFANS account and submit an expense report to the Office of Accounts and Control all unmanaged app purchases that are eligible for reimbursement by the State.
- Submit an expense report to the Office of Accounts and Control and allocate to the agency's RIFANS account all unmanaged app purchases that are eligible for reimbursement by the State.

User

- Comply with all provisions documented in this policy.
- Physically secure the Mobile Device at all times.
- Immediately report any actual or suspected Mobile Device incident, including the loss, theft, or unauthorized access of the Mobile Device, to the supervisor, Service Desk, and/or Chief Information Officer.
- At a minimum, encrypt all sensitive data on the Mobile Device.
- Password protect the Mobile Device with a password that is in compliance with the DoIT Policy 10-01 entitled *Enterprise Password Security* password complexity criteria.
- Enable the password-protected screen locking feature to automatically lock the Mobile Device after a maximum of ten (10) minutes of inactivity.
- Mobile Devices will have up-to-date anti-virus software and the latest security patches installed.
- Do not disclose any sensitive data that is stored on or accessible via Mobile Devices to unauthorized individuals.
- Periodically back up Mobile Device data.
- Do not use any personal email account when conducting State business via email. Use only official State email accounts.

State of Rhode Island Department of Administration Office of Information Technology	V.2.0
	Effective 08/01/2016
Mobile Device Security	Policy 10-04

- Only use a valid State employee email account to create an Apple App Store account.
- Only install unmanaged applications on Supervised Devices that have a valid business use.
- Review all permissions prior to installing any unmanaged application on Supervised Devices.
- Ensure installed unmanaged apps do not adversely affect the operational integrity and performance of Supervised Devices.
- Pay for all costs associated with the download, installation, and on-going use of unmanaged apps that are not eligible for reimbursement by the State.

8. Assistance

Service Desk
ent.servicedesk@ri.gov
 401.462.4357

9. Revision History

Version	Date	Reason for Revision
V.1.0	02/01/2007	Initial version.
V.1.1	04/01/2008	Update.
V.2.0	08/01/2016	Update policy using new format.

This policy is scheduled for review on or before 7/31/2017.

10. Approvals

 Chief Information Security Officer,
 Division of Enterprise Technology Strategy and Services

 Date

 Chief Digital Officer,
 Division of Enterprise Technology Strategy and Services

 Date

 Director,
 Department of Administration

 Date

State of Rhode Island Department of Administration Office of Information Technology	V.2.0
	Effective 08/01/2016
Mobile Device Security Policy User Agreement	Policy 10-04

I have been assigned a Mobile Device to access State of Rhode Island data and information system resources. I acknowledge that, as a condition of receiving a Mobile Device to access State data and resources, I must agree to comply with all provisions of OIT Policy 10-04 entitled *Mobile Device Security* and promise the following, as they relate to the established policy:

1. I will protect against the unauthorized disclosure and/or use of State of Rhode Island assets, sensitive or confidential data, facilities, and information system resources.
2. I will maintain all information resource access codes in the strictest of confidence.
3. I will immediately change any access code that I suspect has been compromised.
4. I will not install any Mobile Wallet Application on the Mobile Device.
5. I will report all activity that is contrary to the provisions of the *Mobile Device Security Policy* and this agreement to my supervisor or the Chief Information Security Officer.
6. I will immediately report the loss of my Mobile Device to my supervisor, Service Desk, or Chief Information Security Officer.
7. I will be responsible for covering the replacement cost of the Mobile Device upon the second and each subsequent occurrence during each 24-month period that I report a Mobile Device assigned to me as being broken, lost, or stolen, whether accidental or not. The 24-initial month period commences on the date that I sign this agreement and expires 24 months from this date. Upon expiring, the 24-month period will automatically renew for a new term of 24 months for as long as I am assigned this Mobile Device.

I have been given a copy of OIT Policy 10-04 entitled *Mobile Device Security* and have read and agree to comply with the policy. I understand that the willful violation or disregard of this User agreement and/or the provisions of OIT Policy 10-04 entitled *Mobile Device Security* may result in disciplinary action, up to and including termination of my employment, as well as any other legal action deemed appropriate, including possible prosecution.

Mobile Device	Device Serial #	State Asset Tag ID #
User Printed Name		SSN (last 4)
User Signature		Date
Approved By		Date