Division of Information Technology

Enterprise Technology Strategy and Services Policy 10-04
Mobile Device Security Policy
Last Revision: 8/28/2020

Brian Tardiff
doa.entsec@doit.ri.gov

1. Purpose

Establish policy for effectively managing and securing mobile devices that store, process, or transmit state data. Establish restrictions and safeguards necessary to secure the state network and data when accessed via mobile devices.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments[1] (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Apple iTunes App Store
Apple's platform for the digital distribution of mobile applications that run on Apple's iOS or OSX operating systems. The Apple iTunes 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. The App Catalog is only available for state-owned Apple iOS or OSX operating system mobile devices. Applications within the App Catalog tend to be business related (e.g. Microsoft Office apps).

Managed App
Applications available for download via the App Catalog on state-owned owned Apple iOS or OSX operating system mobile devices. Any application that can be downloaded via the Apple iTunes App Store but is available for download via the App Catalog is an unmanaged app.

[1] *State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State colleges, the General Treasurer, the Attorney General, or the Secretary of State.*

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 other portable computing devices.

Mobile Wallet
Mobile device software 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).

Supervised Device
A state or personally-owned mobile device that is centrally managed by the state's Mobile Device Management (MDM) solution.

4. Procedures for Compliance

4.1. User Agreement. Mobile device users will be authorized, approved, and have a signed user agreement form prior to using a state or personally-owned mobile device to store, process, or transmit state data and connect to state network resources. Users of state-owned mobile devices will sign the "*Supervised Mobile Device Security Policy User Agreement*" form located on the last page of this policy. Users authorized and approved to use a personally-owned mobile device to access state data and network resources are required to comply with provisions documented in ETSS Bring Your Own Device Security Policy 10-27 and will sign the "*Bring Your Own Device Security Policy User Agreement*" form located on the last page of the policy. Signed user agreement forms will be maintained on file by the agency or ETSS Enterprise Telecommunications Team, as appropriate, in accordance with whom is provisioning the mobile device approved to access state data and network resources (e.g. laptop, tablet, smartphone, iPhone, iPad, etc.)

4.2. Incident Reporting. Incidents involving mobile devices will be handled in accordance with ETSS Incident Handling and Response Policy 10-12. Mobile device users will notify their supervisor and the ETSS Enterprise Service Desk immediately upon becoming aware of an actual or suspected loss, theft, or unauthorized access of a mobile device to report the incident. Once every 24 months, the state will cover the replacement cost of the first occurrence in which a user breaks, loses, or has stolen, whether accidental or not, his/her state provided supervised mobile device mobile. Upon the second and each subsequent occurrence during each 24-month period, the user will be responsible for

covering the replacement cost of the state provided supervised mobile device. The 24-month period commences on the date the supervised 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 supervised mobile device remains assigned to the user. For assistance with incident reporting, please contact:

ETSS Enterprise Service Desk
ent.servicedesk@ri.gov
(401) 462-4357

ETSS Enterprise Security
doa.entsec@doit.ri.gov

4.3. Physical Security.

4.3.1. Physical Access. Mobile devices will always be physically secured, regardless whether or not being used, and physical access will be appropriately restricted (e.g. placed inside a locked cabinet, locked office, behind a locked door).

4.3.2. Unsecured Areas. Mobile devices will not be left unattended within unsecured areas at any time (e.g. non-state facility, publicly accessible area, hotel lobby). Mobile devices will not be left in view of or be physically accessible to others when not being used. Regarding 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 inside a vehicle overnight.

4.4. Data Security.

4.4.1. Data. Only supervised mobile devices are authorized to access and maintain FTI and other confidential data. Mobile device users will not disclose any confidential data that is stored on or accessible via mobile devices to unauthorized individuals. Users should use good judgement and limit the amount of confidential, sensitive, or private data that is stored on mobile devices to only what is necessary to perform required job duties and functions. Data stored on mobile devices will be backed up monthly.

4.4.2. Encryption. Confidential data, including FTI, maintained on mobile devices will be encrypted in accordance with ETSS Data Encryption Policy 05-03. Mobile device data storage drives should be encrypted to ensure the protection of all state data.

4.5. Device Security.

4.5.1. Passwords. Mobile devices will be password protected. Passwords will be configured in accordance with ETSS Enterprise Password Security Policy 10-01. Passwords stored on mobile devices will be encrypted.

4.5.2. Screen Lock. The mobile device password-protected screen lock feature, which requires the user to enter a password to unlock the mobile device, will be enabled. The screen lock feature will be set to automatically lock the mobile device after a maximum of ten (10) minutes of inactivity.

4.5.3. Software. Mobile device users will not install any software on state-owned mobile devices without prior authorization. Mobile wallet software 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.

4.5.4. Anti-Virus/Patching. State-owned mobile devices will have up-to-date anti-virus software and the latest security patches installed. State-owned mobile devices will be scanned to ensure that up-to-date anti-virus software and the latest security patches are installed. Security patches should be installed within two (2) days of the notification of availability. Users are authorized to connect supervised devices to the state wi-fi to download and install mandatory updates.

4.6. Wireless Network Connections.

4.6.1. Authentication. Supervised mobile device 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. Users have no expectation of privacy and will be monitored.

4.6.2. Wireless Access. Supervised mobile device wireless access ports will be disabled when not in use. Bluetooth connectivity will be set to “non-discoverable” mode.

4.6.3. Untrusted Networks. Supervised mobile device 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 necessary and when there is no other alternative, users connecting to a public or private non-state network (e.g. hotel, restaurant, airport, train station, home), either wired or wirelessly, should:

- Enable the firewall on the mobile device.
- Disable file sharing on the mobile device.
- 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).

4.7. Supervised Devices. In addition to the above policy provisions, supervised device users are required to adhere to the following:

4.7.1. Authority. ETSS will manage and maintain authority over all supervised devices. After ten (10) consecutive unsuccessful logon attempts, ETSS will remotely wipe the supervised mobile device. ETSS 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 deemed necessary by ETSS or the user's supervisor. Supervised devices are subject to APRA requests and to recovery by ETSS for the purposes of satisfying those requests. To support recovery of text messaging on supervised devices, an Apple ID will be established by the device issuing authority using the employee state domain email account.

4.7.2. Support. ETSS will not provide support for any issue arising from the use of any installed application, including those available via the App Catalog. Users should be aware that supervised devices have limited memory and are responsible for ensuring that installed unmanaged apps do not adversely affect the operational integrity and performance of supervised devices.

4.7.3. Applications. The only applications pre-approved by ETSS for install on supervised devices are the managed apps available via the App Catalog. All applications available via the Apple iTunes App Store are considered unmanaged applications and should only be installed if there a valid business use justification. Users should be aware that applications often require permissions to access specific functions, provide additional functionality, or enhance the user experience. However, some permissions may 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 that state data is not under an increased risk of being compromised. ETSS 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 of ETSS Technology Acceptable Use Policy 00-02.

4.7.4. Purchases. Apple iTunes 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 that are 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.

4.7.5. Accounts. User accounts created to download applications from the Apple iTunes App Store to supervised devices will be set up using the state employee's email address. Passwords for this account will not the same as any password used by the employee to access any state network resources. 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 email attachments that can be opened by managed apps.

5. Approval / Review Signature

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2020.09.14 08:46:40 -04'00'

Chief Information Security Officer

Supervised Mobile Device Security Policy
User Agreement

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 Stata data and resources, I must agree to comply with all provisions of ETSS Mobile Device Security Policy 10-04 and promise the following, as they relate to the established policy:

1. I will protect against the unauthorized disclosure or use of State of Rhode Island assets, confidential or sensitive 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 unauthorized software nor mobile wallet application on the mobile device.
5. I will report all activity that is contrary to the provisions of this agreement to my supervisor or ETSS Enterprise Security Team at doa.entsec@doit.ri.gov.
6. I will immediately report the loss of my mobile device to my supervisor and ETSS Enterprise Service Desk at ent.servicedesk@ri.gov.
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-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 ETSS Mobile Device Security Policy 10-04 and have read and agree to comply with the policy. I understand that the willful violation or disregard of this user agreement and provisions of ETSS Mobile Device Security Policy 10-04 may result in disciplinary action as well as any other legal action deemed appropriate.

_____ _____

Mobile Device - Name/Type Device Serial #

_____ _____

Mobile Device User - Print Name State Asset Tag ID #

_____ _____

Mobile Device User - Signature Date

_____ _____

Approved By Date