DEPARTMENT OF ADMINISTRATION
Enterprise Policy

DOIT-10-27-2016

DIVISION OF INFORMATION TECHNOLOGY

Bring Your Own Device Security Policy

Date of Last Revision 04/01/2016

Bijay Kumar
(401) 574-9220
bijay.kumar@doit.ri.gov

1. Background

a. The massive increase in mobile computing and personal devices is revolutionizing the end-user experience and forcing many organizations, including public entities, to rethink their business processes. Instead of resisting this wave, it is becoming increasingly commonplace for organizations to allow employees to access organizational systems and data through personally owned mobile devices as a part of performing their job duties. Access to employer systems and data through a personally owned mobile device is convenient for employees, enhances workforce productivity, and offers the possibility of cost savings. However, there are serious risks associated with this model including network risk, privacy risk, legal issues, assurance requirements, and other potential hazards that must be addressed by instituting an effective policy, enforcing technical standards and promoting appropriate end-user awareness.

2. Purpose

a. To establish a Bring Your Own Device Security Policy for the effective management of personally owned mobile devices used to access State networks, applications and/or data and to ensure the confidentiality, integrity, and availability of State networks, applications, and data.

3. Scope

a. This policy covers all State Executive Branch Departments[1] (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.

4. Authority

a. Executive Order 04-06 established the Division of Information Technology ("DoIT") within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive branch of the State of Rhode Island. In accordance with Executive Order 04-06, DoIT will define, maintain, and

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

enforce statewide IT related policies and procedures for the effective use and security of IT resources.

5. **Acronyms and Definitions**

   a. **Agency Head** - An employee's appointing authority or person authorized by the appointing authority or by the Director of Administration to grant agency approval for an employee to participate in the BYOD Program.

   b. **Bring Your Own Device or BYOD** - Refers to the use of a personally owned mobile device to access State networks, applications and/or data.

   c. **BYOD Mobile Device** - A personal mobile device that is being utilized as part of the BYOD Program.

   d. **BYOD Program** - A program piloted by Dolt to permit state employees to use personally owned mobile devices to access State networks, applications and/or data.

   e. **CISO** - The DoIT Chief Information Security Officer

   f. **DoIT** - The Division of Information Technology.

   g. **DoIT Chief** - The individual acting as the head of Do IT as determined by the Director of Administration.

   h. **Mobile Device Management or MDM** - The centralized administration of mobile devices (including personally owned devices) that allows for BYOD policy enforcement, software and application deployment, data backup, device lockout, remote wiping, and more.

   i. **Remote Wiping** - The erasing of data from a mobile device via a remotely sent command. Remote wiping can be targeted (delete only specific accounts, data, or applications) or a full factory reset (delete all device data and reset it to factory settings).

   j. **Root/Jailbreak** - A process (a form of privilege escalation) that removes access permission limitations often placed on mobile devices by the manufacturers and/or service carriers. The end result of this process is that users have administrator-like permissions and are able to perform operations that were previously inaccessible. This process is known as "rooting" (Android devices) and "jailbreaking" (iOS devices).

   k. **User** - An individual who participates in the State BYOD program and uses a personally owned mobile device to access State networks, applications, and/or data.

6. **Policy**

   a. **Eligibility.** In order to be eligible to participate in the BYOD Program, an individual must be a state employee and must be granted authorization by his or her Agency Head and Do IT. In addition, each personal mobile device must be approved prior to being utilized as part of the BYOD Program.

   b. **User Agreement.** Prior to participation in the BYOD Program, prospective Users must read and sign the Bring Your Own Device User Agreement attached hereto as Appendix A. Users will be required to sign an additional Bring Your Own Device User Agreement or revise and sign an existing Bring Your Own Device User Agreement whenever a new personal mobile device is deployed as part of the BYOD Program.

c. **Acceptable Use.** Users must comply with the terms and conditions of DoIT Policy# 00-02 entitled Acceptable Use Policy as may be revised from time to time while accessing State networks, applications, and/or data through a BYOD Mobile Device.

d. **Privacy.** Users have no expectation of privacy when using a BYOD Mobile Device that is connected to the State network. User actions may be monitored and logged.

e. **Reimbursement.** The State will not reimburse Users for any service plan expenses. In addition, the installation of any software required to participate in the BYOD Program may decrease the available memory or storage on a personal device. The State shall not be responsible for compensating the employee for any lost storage space and the State is not responsible for any expenses Users may incur as a result of participating in the BYOD program (e.g. being charged a fee for exceeding data plan limits).

f. **Physical Access.** Users will grant physical access of BYOD Mobile Devices:

   (i.) to DoIT personnel prior to a device being provisioned/deployed as a BYOD Mobile Device, and

   (ii.) when required by authorized State personnel or other authorized entities as a result of a legal hold, a court order, and/or a digital forensics investigation.

g. **Cancellation.** Users will be removed from the BYOD Program upon leaving State employment. Users may be removed from the BYOD Program:

   (i.) due to changes in job positions and/or duties;

   (ii.) at any time if DoIT determines that revoking access is necessary in order to maintain the confidentiality, integrity, and availability of State networks, applications, and/or data; or

   (iii.) at any time the Director of Administration or Agency Head determines that revoking access is otherwise is in the best interest of the State.

h. **Incident Reporting.** Users will notify the DoIT Service Desk, the CISO, and/or their supervisor immediately upon becoming aware that a BYOD Mobile Device is lost or stolen.

i. **Mobile Device Management.** BYOD Mobile Devices will be managed by the State via the use of a small purpose-built application installed on the device. This application also serves as the conduit for accessing State data.

j. **Remote Wiping.** The State has the authority to remotely wipe a BYOD Mobile Device when:

   (i.) the device is reported as lost or stolen;

   (ii.) a User leaves State employment or has a change in job position or duties;

   (iii.) State data is believed to be compromised; and/or

   (iv.) malware or a virus is detected.

   (v.) Unless performing a factory reset type of remote wiping, the remote wiping process should only erase State applications and data from BYOD Mobile Devices. However, there is no guarantee that personal data will not be erased

during the process. The State will not be held responsible for any personal data that is permanently lost or erased from BYOD Mobile Devices for any reason including any data lost as the result of a remote wiping process. It is highly recommended that Users periodically back-up personal data stored on BYOD Mobile Devices.

k. Support. Only the Android and iOS mobile device platforms are approved for the BYOD Program. Due to the increased security risk, mobile devices that have been "rooted" (Android) or "jail broken" (iOS) will not be approved for the BYOD Program. DoIT will not support any BYOD Mobile Devices beyond the installation of applications required for participation in the BYOD Program.

l. Passwords. BYOD Mobile Devices will be password protected. Passwords will comply with requirements documented in Do IT Policy# 10-01 entitled Enterprise Password Security as may be revised from time to time. BYOD Mobile Devices that are unable to meet these requirements will have passwords that are as complex as possible for the particular device. After 15 contiguous unsuccessful password attempts, BYOD Mobile Devices may be remotely wiped.

m. Screen Lock. Users will enable the password-protected screen locking feature on BYOD Mobile Devices. The screen lock will be set to automatically lock the BYOD Mobile Device after 2 minutes of inactivity.

n. Software. BYOD Mobile Devices will have up-to-date anti-virus software and the latest security patches installed. Only applications available via Google Play (Android) and iTunes (iOS) may be installed on BYOD Mobile Devices. However, DoIT reserves the right to prohibit any application from being installed on BYOD Mobile Devices, including those available via Google Play and iTunes. Non-compliant BYOD Mobile Devices may be revoked from participating in the BYOD Program.

o. Data. All sensitive and/or confidential State data stored on BYOD Mobile Devices will be encrypted at all times. Users will not disclose or share any State data that is stored on, or accessible via, BYOD Mobile Devices to unauthorized individuals or unauthorized devices.

p. General Security Practices. Allowing Users to access State networks, applications, and data through BYOD Mobile Devices imposes an increased risk to the State of sensitive and/or confidential data being compromised. To reduce this risk, Users should secure their BYOD Mobile Devices as best as possible at all times (this is especially critical when not in a trusted location). Although not all-inclusive, the following security practices should be observed by Users at all times:

(i.) do not connect to untrusted networks;

(ii.) disable wireless access when not in use and set Bluetooth to "non-discoverable" mode;

(iii.) physically secure BYOD Mobile Devices out of view of others when not in use;

(iv.) do not leave BYOD Mobile Devices inside a vehicle overnight; and

(v.) do not leave BYOD Mobile Devices unattended at any time when in use.

q. Policy Reviews. This policy will be reviewed annually and updated as required.

r. Noncompliance. Any employee who willfully violates this Policy may be subject to disciplinary action up to and including termination of employment.

s. Waivers. The Agency Head 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 Head 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 DoIT Chief. Waivers expire one year from date of issue, or upon the ending for the reason of the waiver, whichever occurs sooner. The DoIT Chief shall have the authority to renew or rescind any waiver granted pursuant to this section.

t. Standards and Procedures. The CISO and DoIT Chief may approve and adopt Procedures to effectuate the purpose of this Policy. Any Procedures adopted pursuant to this section should be fluid in nature to allow for timely adjustments and improvements.

u. Amendment. This Policy may be amended or rescinded at any time without further notice.

7. Roles and Responsibilities

a. *Chief Information Security Office*

(i.) Periodically review and update this Policy, as required.

(ii.) Periodically assess BYOD procedures to ensure compliance with this policy.

(iii.) Provide periodic BYOD security awareness and training, either in-person or online.

(iv.) Follow up on BYOD Mobile Devices that are reported lost or stolen.

b. *Agency*

(i.) Ensure User has a signed Bring Your Own Device User Agreement on file prior to being approved for the BYOD Program.

(ii.) Ensure User has signed the Bring Your Own Device User Agreement prior to deploying each personal mobile device.

(iii.) Install any software/applications required for participation in the BYOD Program.

(iv.) Verify that the personal mobile device has a password, that the phone screen locks, that State data is encrypted, and that the User has access.

(v.) Contact the CISO to report a lost or stolen BYOD Mobile Device.

c. *User*

(i.) Comply with provisions documented in this Policy.

(ii.) Read this Policy and the Acceptable Use Policy and execute the Bring Your Own Device User Agreement prior to participating in the BYOD program.

(iii.) Notify DoIT and supervisor immediately upon becoming aware of a lost or stolen BYOD Mobile Device.

(iv.) Create DoIT compliant password and enable screen lock on the BYOD Mobile Device.

(v.) Keep personal BYOD Mobile Devices physically and logistically secure.

(vi.) Do not disclose or share any State data stored on, or accessible via, BYOD Mobile Devices to unauthorized individuals or unauthorized devices.

8. Signatures

Chief Digital Officer, Office of Digital Excellence/
Head of the Division of Information Technology

3/29/16
Date

Chief Information Security Officer,
Division of Information Technology

3/30/2016
Date

Director, Department of Administration

3/29/16
Date