State of Illinois
Department of Innovation & Technology

Mobile Device Security Policy

Contents

OVERVIEW 1
POLICY PURPOSE 1
GOAL 1
SCOPE 1
DEFINITIONS 2
ENFORCEMENT 3
POLICY 3
RESPONSIBILITY 6
POLICY COMPLIANCE 7
AUTHORITIES, GUIDELINES OR SOURCES 7
REVISION HISTORY 7

POLICY OVERVIEW

The Department of Innovation & Technology (DoIT) seeks to protect State of Illinois (State) information, systems and records from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

POLICY PURPOSE

The purpose of the Mobile Device Security Policy is to describe the minimum security policy for remote access to State information and systems both from State-owned and User-owned Authorized Mobile Devices. All Authorized Devices used to access State information and systems must be appropriately secured to prevent unauthorized access and to prevent confidential data (as defined in the Data Classification Policy) from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the State of Illinois' computing and information infrastructure.

GOAL

The goal of Mobile Device Security Policy is to create a consistent, secure, and operationally effective set of parameters within which users of State-owned or User owned (and used for State purposes) mobile devices can utilize those available communication devices while simultaneously adhering to a best practice based approach to preventing unintended consequences, security risks and other negative outcomes that interfere with successful achievements of the mission of the State of Illinois.

Mobile Device Security Policy

SCOPE

This Policy applies to any Authorized Mobic Device, owned either by the State or by a User, which is used to remotely access State information and systems. The procedures underlying this policy will be reviewed and updated every 365 days, and the policy will be reviewed and updated every three years. This policy applies to all personnel in State of Illinois agencies under the Executive Branch.

DEFINITIONS

Definitions for terms used in this policy can be found in the *DoIT Terminology Glossary* located on the DoIT web page under Support/Policies. The terms and definitions listed below are meaningful for this policy. In the event of conflict between the definition in the *DoIT Terminology Glossary* and the definition contained in this policy, the definition below shall control for this Policy.

1. **User:** Anyone with authorized access to State business information systems, including, but not limited to, permanent and temporary employees or third-party personnel such as contractors, and consultants.

2. **Mobile Devices:** These include, but are not limited to, any portable cartridge/disk-based, removable storage media (e.g., compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory), or any mobile computing and communications device with information storage capabilities (e.g., notebook/laptop computers, tablets, public internet access devices, personal digital assistants, smart phones, cellular telephones, etc.).

3. **Authorized Mobile Device:** Any Mobile Device authorized by State management to be used to connect to State network resources or contain State data. A Mobile Device that is owned by the User can become an Authorized Mobile Device pursuant to this Policy, and may be referred to as a "Bring Your Own Device" or "BYOD" option. Mobile Devices, regardless of ownership, which are not Authorized are prohibited from connecting to the State network, IT infrastructure or resources, and must not store, contain or transmit State data.

4. **Screen Lock:** A software mechanism used to hide data on a visual display while the computer or device continues to operate. A screen lock requires authentication before a User can access organization resources.

5. **Screen Timeout:** A mechanism that will automatically lock idle Devices or end a session when the Device has not been used for a specified time period (e.g., 5 minutes).

6. **Encryption:** The process of transforming information or messages in such a way that only authorized parties can read it.

ENFORCEMENT

Participation in the BYOD option is voluntary. Users who select BYOD option voluntarily agree to comply with all provisions of this policy as applied to User-owned Mobile Devices.

Both State-owned and User-owned Mobile Device Users understand that noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, and may subject the User to civil or criminal penalties, litigation, restitution, fines, and/or other consequences or penalties.

POLICY

1. All Authorized Mobile Devices must be approved by an authorized Agency representative and approved by DoIT to transmit, receive, store, or process State information.

2. As a prerequisite to using an Authorized Mobile Device, Users must receive, read, and formally agree to comply with this Policy before authorization is granted to ensure the User is aware of the risks and procedures associated with this privilege.

3. The State retains the right to refuse Authorization of a User's Device, and/or to discontinue the support of a previously Authorized Mobile Device. If a User is provided a State-owned Authorized Mobile Device similar to an existing BYOD device, then the similar BYOD device will be removed from having access to State data and will no longer be eligible as an Authorized Mobile Device.

4. Communications on all Authorized Mobile Devices, regardless of ownership, are not presumptively private. DOIT may monitor any Authorized Mobile Device for the security and administration of State data. While DOIT will generally attempt to only monitor communications strictly related to State business on a User-owned Authorized Mobile Device, and to limit any such monitoring to the minimum required to achieve its legitimate security and administrative needs, technological and practical constraints may result in the capture or monitoring of personal information on a User-owned Authorized Mobile Device. As a result, every User of an Authorized Mobile Device acknowledges and agrees that the User has no reasonable expectation of privacy for any Authorized Mobile Device, whether State-owned or User-owned.

5. Participation in the BYOD option is voluntary and no User will be required to use their own device for the purpose of conducting State business unless they voluntarily agree to participate in the BYOD option. However, all Users must agree to immediately upon request temporarily turn over to the State any Authorized Mobile Device, including a User owned Device, when security incidents occur and/or for the installation of required software to protect State systems. The benefit of using a User-owned Authorized Mobile Device for State business is inextricably linked to the risk the Device will need to be temporarily turned over and its contents copied for legal purposes, including, but not limited to, FOIA requests for state information, legal hold or litigation hold notices, law enforcement requests, subpoenas, etc. The risk of participating in the BYOD option also includes the possibility the telephone number for a User-owned Authorized Mobile Device may become publicized.

6. The State is not responsible for any software, data, or hardware problems with, or the loss, damage, or theft of, any User-owned Authorized Mobile Device. The State will not provide any reimbursement for State business-related data/voice plan usage on any User-owned Authorized Mobile Device, or for hardware or device upgrades.

7. Certain State approved and installed software and/or applications are a prerequisite to use of an Authorized Mobile Device, whether User-owned or a State-owned. Users must accept and not delete, remove, modify, disable, or otherwise alter any third-party software that is provided by or installed by the State on any Authorized Mobile Device.

8. The State retains the right to quarantine an Authorized Mobile Device, and to prevent the download of, delete, or require the deletion of any unauthorized third-party software or applications on any Authorized Mobile Device to achieve the State's legitimate security and administrative needs, regardless of whether it is a State-owned or a User-owned device.

9. The User understands and accepts the risk of having data, files, and/or applications, including personal files or applications, on the Authorized Mobile Device deleted by the State to effectuate the State's legitimate security and administrative needs if malware or viruses are detected. Accordingly, the State recommends that a User-owned Authorized Mobile Device should be backed up on the User's own hardware or system with sufficient regularity to protect the User's personal data from this risk.

10. Users must comply with all applicable State password policies on Authorized Mobile Devices, including on User-owned Authorized Mobile Devices. This includes the use of strong passwords, password expiration, and password history limitations.

11. Authorized Mobile Devices must, when applicable, enable screen locking and screen timeout functions in combination with a password or passcode for protection.

12. The physical security of every Authorized Mobile Device is the responsibility of the User. Authorized Mobile Devices shall be kept in the employee's physical presence whenever possible. Whenever an Authorized Mobile Device is being stored, it shall be stored in a secure place, preferably out-of-sight.

13. If an Authorized Mobile Device is lost or stolen, User shall immediately, but no later than 24 hours, report the incident to the DOIT Help Desk, law enforcement and his or her supervisor.

14. If an Authorized Mobile Device is lost or stolen, DOIT reserves the right to remotely wipe the Device of any and all State data stored on the Authorized Mobile Device. While the State will use reasonable efforts to delete only State data, the User acknowledges the possibility and accepts the risk that all data, including personal data, could be wiped in some circumstances.

15. State-owned Authorized Mobile Devices should be kept in provided protective cases whenever possible. If a State-owned Authorized Mobile Device is damaged because it was not kept in the provided protective case, the User's Department Director or a delegate may require User to reimburse the State for the cost of repair or replacement.

16. State data, software, and applications must be removed from a User-owned Authorized Mobile Device utilizing DOIT-approved procedures before the Authorized Mobile Device is returned, exchanged, sold, disabled, or otherwise disposed of, and before a User leaves State employment.

17. Authorized Mobile Devices shall have connectivity limited to State resources on an as needed basis, and in accordance with the IT Resource Access Policy. Individual Agencies reserve the right to implement a more restrictive connectivity policy.

18. Every State-owned Authorized Mobile Device used to gather, process or store Personal information (as defined by the Personal Information Protection Act - 815 ILCS 530) shall be equipped with full-disk encryption. Users of these Devices are the data owners, and must ensure the confidential data is encrypted while stored on the Device.

19. It is a violation of this Policy for any User to attempt to bypass, penetrate, alter the configuration of, or to otherwise affect the operation of any encrypted storage media.

20. The State retains the right to filter and track web access on any State-owned Mobile Device.

21. Any User conducting State business on User-owned Authorized Mobile Devices must do so only via the User's State email account.

22. State email accounts must not be used to engage in prohibited political activity (as that term is defined in the State Officials and Employees Ethics Act (5 ILCS 430/1-1 *et seq.)*) at any time, and this prohibition continues to apply to the use of State email accounts, regardless of the means of access, including State-owned and User-owned Mobile Devices.

23. The use of State email on a User-owned Authorized Mobile Device is subject to the same restrictions, limitations, and monitoring as covered by other applicable policies and laws.

24. The use of text messaging, instant messaging, or any other related communication method/application to conduct any State business on an Authorized Mobile Device is strictly forbidden.

25. The use of State-owned telephones is the primary and preferred method for conducting telephone communication for State business. State business should only be conducted by telephone on a User-owned Mobile Device when a State-owned telephone is not reasonably available.

26. The State can employ or enable geolocation services on State-owned Authorized Mobile Devices to effectuate the State's legitimate security and administrative needs, and these functions and settings must not be disabled or modified in any way by the User.

RESPONSIBILITY

1. Each User of an Authorized Mobile Device used to remotely access State information and systems is responsible for following this Policy and any related policy or procedure promulgated by the head of his or her Agency.

2. Each Agency may establish policies and procedures and assign responsibility to specific Agency personnel to achieve compliance with this Policy.

3. Anyone observing what appears to be a breach of security, a violation of this policy, a violation of state or federal law, theft, damage, or any action placing State information and systems at risk must immediately report the incident to an appropriate level supervisor, manager, or security office within their organization.

4. Managers and supervisors are responsible for ensuring that Users are aware of and understand this policy and all related policies and procedures.

Mobile Device Security Policy

POLICY COMPLIANCE

In order to implement this Policy, the Department of Innovation & Technology establishes procedures and designates responsibility to specific personnel. To the extent necessary, each Agency must establish procedures in order to achieve policy compliance. It is the responsibility of all authorized users of IT Resources to understand and adhere to this Policy. Failure to comply with this policy could result in discipline, up to and including discharge.

AUTHORITIES, GUIDELINES OR SOURCES

None

REVISION HISTORY

Original effective Date:	September 8, 2015
Last Review date:	October 26, 2016
Revised date:	November 2, 2016

Through the signature reflected below, the Secretary of the Department of Innovation & Technology provides management commitment to this policy.

Effective upon latest signature below

Department of Innovation & Technology Approvals

Date: 11/10/16

DoIT Secretary, Hardik Bhatt

Date: 11/9/16

DoIT General Counsel, Michael Basil