Policy and Procedures for Use of Personally-Owned Mobile Devices to Access the Information Resources of Indiana State Government: A Semi-managed BYOD Program

TABLE OF CONTENTS

LIST OF TABLES

Policy Background and Context

The purpose of this policy is to define accepted practices, responsibilities and procedures for the use of personally-owned mobile devices, including mobile phones, smart phones and tablets, that the Indiana Office of Technology (IOT) authorizes to connect to enterprise systems. The central concept of this policy is that the employee, through an opt-in decision, trades some control over his or her personal mobile device to access enterprise resources (such as the network or email). It is important that the consequences and obligations of this arrangement are well-understood. These obligations include, but are not limited to:

- Employee acceptance that a personal device may be remotely wiped (i.e., erasing State-only or, if needed, all data and applications) by IOT as part of its data sanitization requirements
- Employee understanding that he or she is solely responsible for backing up any personal content on the device, as that information cannot be guaranteed to be protected by selective wipes
- Employee agreement to keep the device updated and in good working order
- Employee accepts that IOT will set the standards for operating system and application version control and agrees to abide by those standards.
- Employee acknowledgment that IOT and its agents will in no way be responsible for damaged, lost or stolen personal devices while the employee is performing organizational business
- Employee agreement to allow IT to load a mobile device management software agent and any other software deemed necessary by the organization on personally owned devices upon the organization's request
- Employee acceptance that enterprise work may be tracked to meet the legal and fiduciary responsibilities of the State of Indiana and its agents
- Employee understanding that participation in the BYOD program is voluntary, and by no means constitutes a request by the State of Indiana, direct or implied, to conduct enterprise business on the personal mobile device outside of predetermined and regularly scheduled business hours.

It is the policy of IOT to protect and maintain the security and privacy of state information assets. The use of mobile devices supplied by State agencies shall be primarily for enterprise business. However, IOT will permit the use of personally owned devices, subject to the following broad guidelines:

- The decision to be eligible to use a personally owned mobile device for organization business will be based on a documented business need and appropriate management approval. Guidelines for eligibility are in Appendix A.
- Reimbursement of expenses incurred by qualified users will follow agency policies.

Definitions

BYOD

The acronym “BYOD” stands for Bring Your Own Device” and applies …

Smartphone

A smartphone is a mobile device that includes cellular voice, messaging, scheduling, email and Internet capabilities. Smartphones may also permit access to application stores, where aftermarket ‘apps' can be purchased. The smartphone vendor may have a software developer kit that allows developers to use native APIs to write applications. Examples include iOS, Android and Windows Phone.

Tablet

A tablet is a mobile device that has a touchscreen display typically larger than that of a smartphone and includes messaging, scheduling, email and Internet capabilities, with no cellular voice capabilities. Tablets like smartphones also permit access to application stores, where aftermarket ‘apps' can be purchased. The tablet vendor may have a software developer kit that allows developers to use native APIs to write applications. Tablet device subtypes include slates (no standard keyboard), and hybrids (detachable keyboard). The primary use is the consumption of content, however as apps mature content creation on tablets is becoming commonplace.

Mobile Device

This refers to any mobile phone, smartphone, tablet or hybrid device.

Mobile Applications

This refers to software designed for any or all of the mobile devices defined in this policy.

Scope

This policy applies to all users, (e.g., employees, contractors, consultants, and customers who access and/or use the State of Indiana’s IT resources from non-State of Indiana issued and owned devices.

User Roles and Responsibilities

User Responsibilities

Despite individual ownership of the mobile device, IOT expects the user to assume certain responsibilities for any device that contains State of Indiana information or connects to **State of Indiana** resources. Users must ensure that they comply with all sections of this agreement.

Conditions

- Users are required to enroll their device(s) into the mobile device manager environment in use by IOT and maintain their devices in compliance in order to access enterprise systems hosted or contracted by IOT.
- Users are limited to enrolling 2 concurrent mobile devices with the organization at any one time.
- Users must maintain a device compatible with the organization's published technical specifications (defined in Appendix B). IOT will periodically review the suggested specifications and, based upon security and support requirements, makemodifications. All modifications will be communicated to the intended audience if the modification affects a number of devices currently in use. These modifications could result in a decrease in functionality or support until the device is upgraded or updated. In rare cases, extreme security flaws or findings may dictate a total loss of access until the device again meets standards.
- A baseline security set will be enforced on the device. Any modifications or changes to the baseline security set on the device will cause the device to be out of compliance. If a device falls out of compliance, then it may be blocked from access until it meets minimum security requirements.

Loss or Theft

- Upon loss or theft of a device, users must submit a report to the HelpDesk. This allows the device to be remotely wiped over the network before cancelling anymobile operator services.
- The act of remotely wiping data from the device does not cancel the service in effect for the device. It shall be the user’s responsibility to contact their carrier and cancel any individual voice and data services after the remote wipe ofthe device is completed.

Violations & Uncertainty

Users shall report violations of this agreement to his/her manager or IOT’s Chief Information Security Office upon learning of such violations. If a User is uncertain whether an activity is permissible, s/he will refrain from the activity and obtain authorization from the manager before proceeding.

Applications and Downloads

- Users must ensure that they install application updates in accordance withIOT guidelines.

- Users may download and install applications from the platform's public application store as long as the application complies with this policy and the IT security policy. Approved public application stores:
    - Apple – Apple App Store/Itunes
    - Android – Google Play Store
    - Windows – Windows Store
    - Amazon – Amazon App Store

Backup and File Sharing or Synchronization

- Users are responsible for backing up all personal information on their personal hard drives or other non-State-owned backup systems. State of Indiana andits agents cannot be held liable for erasing user content and applications when it is deemed necessary to protect enterprise information assets or if a wipe is accidentally conducted.
- Users must use enterprise-sanctioned network file shares for the purpose of synchronizing State of Indiana information between devices, and may onlyuse approved cloud storage providers.
    - Approved cloud storage providers:
        - Syncplicity
        - OneDrive for Business (requires SharePoint Online license. Please see http://www.in.gov/iot/files/OneDrive_for_Business_Policy_16-01.pdf for more information)
- Users are prohibited from sending State of Indiana information to a personal external email address.

Functionality and Feature Management

- Upon IOT's request, users must allow the installation and/or update of themobile device management software agent, and any necessary add-ons pertaining to the mobile device management software agent, on the user's device.
- The device functionality must not be modified unless required or recommended by IOT or by the mobile carrier as agent of IOT.
- The use of devices that are “jailbroken”, "rooted", or have been subjected to any other method of altering or disabling built-in protections or compromising in any way the device operating system, is not permitted and constitutes a material breach of this policy.
- Users must accept that, when connecting the personal mobile device to State ofIndiana resources, IOT's security policy will be enforced on the device. The security policy implemented may include, but is not limited to, policy elements such as passcode, passcode timeout, passcode complexity and encryption.
- Users must accept that, when connecting the personal mobile device to State ofIndiana resources, IOT will establish and enforce standards for operating system and application version levels and will from time to time require users to update the operating system or applications to approved versions.
- Users must accept that IOT has the right to wipe the device if it is lost, stolen, retiredor otherwise compromised, or when a separation or layoff from employment occurs.
- Users are solely responsiblefor backing up any personal content on the device, as that information cannot be guaranteed to be protected by selective wipes.

- Users must take appropriate precautions to prevent others from obtaining access to their mobile device(s). Users will be responsible for all transactions made with their credentials, and are prohibited from sharing individually assigned passwords, PINs or other credentials.
- Users are responsible for promptly, and without alteration, bringing or sending the mobile device to the IT security department and handing over necessary deviceaccess codes upon notification that the device is needed for discovery or other litigation purposes.
- Users may not provide access credentials for devices connected to the State ofIndiana internal systems to any other individual, and each device in use must be explicitly granted access after agreeing to the terms and conditions of this document.

User Privacy

Through mobile device management software installed on a user's device the organization gains a level of access to the personal device that could potentially enable it to obtain access to private information, such as location, phone number, application inventory, make\model and carrier. IOT has put in place appropriate physical, electronic and managerial procedures to restrict access to this private information to a limited set of administrators.

Indiana Office of Technology's mobile device management software does not collect keystroke activity or the internal content of installed applications.

Data and System Security

All organization data that is stored on the device must be secured using IOT’s mandated physical and electronic methods at all times. Users must take the following physical security preventative measures to protect State of Indiana data and systems.

- All users shall abide by IOT standard information security directives for the device atall times.
- Device users must comply with directives from IOT to update or upgrade system software and must otherwise act to ensure security and system functionality. Users must also adhere to IOT mandates to delay system software upgrades when presented with a formal instruction, until noted otherwise.
- Personally owned mobile devices connecting to the network must meet thesecurity criteria listed in Appendix C.
- Mobile devices must not be left unsecured or unattended, even for a short periodof time.
- Mobile devices must not be left in a vehicle overnight.

- A mobile device displaying sensitive information being used in a public place (e.g., train, aircraft or coffee shop) must be positioned so that the screen cannot be viewed by others, thus protecting State of Indiana information. A tinted/polarized screen guard may be used to decrease the viewing angles of any mobile device.

There are consequences for end users who do not comply with the policies detailed in this document:

Any inappropriate use of Information Resources or failure to comply with this agreement may result in disciplinary action, up to, and including immediate dismissal from employment, criminal prosecution where the act constitutes a violation of law, and an action for breach of contract if applicable.

Non-exempt state employees may be disciplined for using mobile devices to perform work, including reading or responding to email, phone calls, text or voice messages, beyond the regularly assigned work hours or while on leave unless the employee has been specifically and explicitly authorized by the appropriate management official to perform that additional work at that time.

Technical Support Processes

How to Get Support

The IOT HelpDesk will provide BYOD support to assist users in enrolling their device in the mobile device manager. Users can access self-support tools and FAQs at http://www.in.gov/iot/2605.htm. The HelpDesk will not support device replacement, device upgrade, device operational questions or embedded software operational questions (such as questions related to the browser, email system, etc.). The help desk will only provide assistance on questions related to Indiana Office of Technology back-end software and the delivery of State of Indiana content to the device. All other inquiries must be directed to the end-user's mobile operator or other issuing retailer supporting the personal device.

Warranty and Replacement Responsibility

If an employee's device breaks or becomes damaged while conducting enterprise business, neither the State of Indiana, nor its agents, will reimburse the employee for any repairs or replacements. Consult with your device's manufacturer or retailer for applicable warranty agreements or repair services.

The employee is responsible for notifying the help desk prior to sending their device for repair or replacing their personal device. Upon notification, Indiana Office of Technology will perform a factory reset on the device. This process will remotely wipe all data natively stored on the device and return it to factory default settings. It will be user’s responsibility to back up personal applications and data prior to this event.

Miscellaneous

Termination of Employment

Upon termination of employment, IOT will perform a selective wipe of Indiana applications and data from all devices where possible. Should a selective wipe be not possible, IOT will perform a complete wipe of all devices with the organization's information on them. It is the user's responsibility to back up personal application and personal data (only) prior to this event, and to restore only personal information after the device has been cleared of contents. Users must confirm the removal of any State of Indiana data and any backups thereof from the personal mobile device, before any payment of severance, pension or other compensation can be dispensed.

Individuals are not authorized to restore any application or data that originated through the relationship with the State of Indiana. Any attempt to restore such information will be subject to legal action against the individual.

The help desk will verify that all organization-related information has been removed.

Terminated employees must sign off on having no other copies of State of Indiana information stored on their devices.

NOTE: Provisions in the employee agreement related to the handling of enterprise information also pertain to such handling on personal devices or the backups of the devices, regardless of media.

Exceptions

Security exceptions will be determined by and should be routed to the IT security department. Exceptions to this policy ultimately may only be approved by the CIO.

Investigations and Litigation

In the event of the State of Indiana or its agents needing access to the device for investigatory, discovery or other purposes in litigation, the employee is obliged to hand over the device along with the necessary passcodes.

Related and Other Documents

IOT also developed and instituted an Information Security Framework (ISF) that applies to all state agencies supported by IOT. The ISF sets policy, establishes control objectives and controls and references practices that secures Indiana government information assets.

The practices referenced in the Information Security Framework can be accessed by members of the State of Indiana Network through the following link: http://www.in.gov/iot/2339.htm

User Agreement

By accessing Indiana State information resources and data, you acknowledge that you have read this document in full and understand the terms of use and your responsibilities as a designated user. You agree to these terms in their entirety and agree to fully, and to the best of your ability, comply at all times to the responsibilities contained herein.

Furthermore, you agree to make no claims on your organization to protect any personal data and fully understand that you have accepted this policy under no coercion of any kind from your employer.

Finally, you understand that violations of this agreement can result in revocation of BYOD eligibility and subject you to *potential disciplinary actions, up to, and including, termination of program eligibility.*

The Indiana Office of Technology can, at any time and at its discretion, modify this user agreement. Continued use of Indiana information resources and data signifies your acceptance of any changes to this agreement.

Appendix A: Guidelines for Eligibility

- There is a justifiable business requirement for having mobile access to State of Indiana information.
- The user agrees to opt in to Indiana Office of Technology management policies and procedures defined here and in related policy documents.
- The user's device satisfies the conditions listed in Appendix B and Appendix C.

Appendix B: Eligible Devices and Platforms

The following device and platform types are eligible for the BYOD program (see Table 1). These choices are subject to change at any time. Users should check periodically for updates at [insert intranet URL]. Users will be notified if their devices are automatically detected as no longer being eligible.

Table 1. Eligible Devices and Platforms

Platform	Device	Software Version
Android	N/A	5.0.0 or higher
IOS	iPhone\iPad	11.2.2 or higher
Windows	N/A	Windows Phone 8

Appendix C: Security Criteria for Personally Owned Mobile Devices

All personally owned mobile devices connecting to the network or accessing organization information must meet the following security criteria:

- All users of State of Indiana resources must select strong passwords and change passwords in accordance with the Indiana Office of Technology password management policy.
- All personal mobile devices must be configured with a minimum password length of six alphanumeric characters.
- All personal mobile devices must be secured with a password-protected screen saver when left unattended, and must be configured to automatically lock after a predefined period of inactivity.
- The mobile device management (MDM) tool, MobileIron, which has been approved by the Indiana Office of Technology must be installed on the device.