MOBILE DEVICE POLICY

Policy Number: Operations (ITP) 07-04

Issue Date: January 31, 2012
Effective Date: January 31, 2012

1. Purpose

Establish requirements for mobile devices in order to connect to the State's backbone via cellular or similar technology.

2. Revision History

Revision Date	Revision Number	Change Made	Reviser
05/04/2007		Creation of Policy	J. Kuntz
05/04/2007	01	Eliminate separate policy for Blackberry and include the product in Mobile Device Policy	J. Kuntz
05/17/2007	02	General Revisions	R. Bauchle
1/31/2012	03	Addition of Policy governing Digital Tablets	Technology Roadmap Committee
06/10/2013	04	Removed "Mobile Device Guidelines" and replaced with "this policy" and updated Mobile/Smartphone standard.	M. Hicks
5/6/2016	05	Addition of MobileIron requirements and other general revisions	J. Stipe
2/16/2017	06	Updated responsibilities section.	J. Stipe
4/24/2020	07	Changes made to reflect changes in overall mobile environment	J. Stipe et al.

3. Persons, Groups, Systems Affected

All agencies within the Executive Branch of Indiana State Government and those connected to the State backbone.

4. Policy

IOT will ensure that all mobile devices meet state security standards and technological architecture. All personally owned mobile devices used to access State of Indiana information resources, including wireless phones, tablets and other wireless materials are subject to compliance with the policy statements in the Indiana Resource Use Agreement (IRUA) and the Policy and Procedures for Use of Personally- Owned Mobile Devices to Access the Information Resources of Indiana State Government: A Semi- managed BYOD Program, published separately. All agencies will follow the implementation guidelines and procedures outlined in this policy when attempting to gain remote access to the State's backbone. Failure to follow the guidelines could result in disconnection from the state backbone and the disabling of the mobile device.

Mobile devices must be secured in accordance with the Information Security Framework. The details for Information Security Framework can viewed at:
http://www.in.gov/iot/files/Information_Security_Framework.pdf.

5. Standards

Tablet – Apple iPad will be the State of Indiana supported standard for tablet devices and will be available for State purchase. Android tablets will be supported on a "best effort" basis. Windows tablets will be allowed through the Desktop/Refresh department and will be managed in Active Directly whereever possible.

Mobile / Smart phones – Apple iPhone is the State of Indiana default standard for mobile/smart phone devices. All FirstNet devices will primarily be supported through the AT&T FirstNet Helpdesk. Android phones will be supported on a "best effort" basis.

6. Responsibilities

6.1. For state approved and supported purchases, end users will only purchase mobile devices as represented insection 5. Standards.
6.2. The storage of sensitive information, such as tax data, child and family services, health data, and other personal data on a mobile device shall not be permitted.
6.3. All mobile devices used to access State of Indiana information resources shall be properly enrolled and in compliance with the State's mobile device management platform. Password policies, encryption requirements and requirements compliance are expected to be used by end users/customers and will be enforced by the mobile device management platform.
6.4. All mobile devices accessing the state backbone are required to have a virus protection software application in operational mode (where available).
6.5. End users are required to report the loss of state purchased devices and any personal devices given access to the State network that may have personal information at the time of the device being lost.
6.6. At no time should any State of Indiana employee provide their login or email password to anyone, not even family members. Passwords are NEVER to be shared! The State of Indiana employee bears responsibility for the consequences should the access be misused.

7. State Environment Protections

7.1. IOT will provide mechanisms for mobile device management and password, encryption, and compliance enforcement for all mobile device types
7.3. All hosts that are connected to State of Indiana internal networks via remote access technologies must use the most up-to-date anti-virus software (where available).
7.4. IOT will manage centralized security implementation for all wireless technology.
7.5. IOT will deploy configuration control and management to ensure the latest software releases and security features are available on mobile devices accessing the State of Indiana network backbone.

8. Definitions/References

Statutory Authority: IC 4-13.1
Fair Information Practices; Privacy of Personal Information chapter, this definition in IC 4-1-6-1(b): "Personal information" means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or his presence, registration, or membership in an organization or activity or admission to an institution.

9. Support Items

9.1. Development and Support of the applications: State purchased mobile devices will be managed through IOT. IOT will maintain necessary Apple authorizations and management of the *submittal* of agency developed applications for publishing.
9.2. Internal development of applications will be the responsibility of agencies. IOT will provide publishing support with Apple.
9.3. Remote wipe of information on the mobile devices will be performed when the device is reported lost. This would include all mobile device data on State-owned or personal device.
9.4. Managing purchases and types of applications loaded on to the devices will be joint responsibilities between IOT and agencies.
9.5. IOT will maintain defense strategies against third-parties access to devices and malware being placed on the devices.