BYOD Policy Release

Joanne E. Hale, PhD

Acting Secretary of Information Technology

Office of Information Technology

June 23, 2016

Agenda

Opening Remarks	OIT, Sec. Joanne Hale
- *Importance of BYOD governance*	
Presentation Overview	OIT, Mason Tanaka
- *Overview of overall agenda*	
BYOD Governance	OIT, Mason Tanaka
- *Policy (to include non-state AD forest responsibilities)*	
- *User Agreement Form*	
- *Policy Effective Date and Compliance Date*	
Q&A - BYOD Governance only	OIT, Mason Tanaka
MaaS360 Overview & Demo	IBM, Phil LaDuke
- *Overview of tool*	
- *Demonstration of tool*	
Q&A – MaaS360 only	IBM, Phil LaDuke
ISD Administration (State AD Forest)	ISD, Mike Vanhook
- *How ISD is going to administer program*	
- *State Email device partnerships require connection*	
- *Agency admin/reporting requirements and process*	
ISD Service (State AD Forest)	ISD, Mike Vanhook
- *Availability*	
- *Cost*	
- *How do agencies acquire subscription*	
Q&A – ISD Admin and Services only	ISD, Mike Vanhook
Open Floor	All

BYOD Governance

Governance for the Use of Personally Owned Mobile Devices

Presented by: Mason L. Tanaka
Assistant Secretary of Information Technology
Office of Information Technology
Presented on: June 23, 2016

BYOD Workgroup

Hornsby, Debbie - CHAIR	Revenue – ITD
Alexander, John	Revenue – ITD
Bess, Art	Finance – ISD
Bird, Brad	Finance – ISD
Cook, Joel	Finance – ISD
DuBard, Derik	Finance – ISD
Gallacher, John	Conservation – IT
Gaston, Drew	Finance – ISD
Green, Mark	Agriculture – IT
McCanless, Donald P.	Medicaid – IT
Rainey, David	Rehab – IT
Schodorf, Robert	Finance – ISD
Segrest, Lane	Agriculture – IT
Vilamaa, Kristopher	Mental Health - IT
Williams, Joshua L.	Finance – ISD
Williamson, Pam	Revenue – ITD
Winborne, Ellis	Finance – ISD
Worden, Melissa	Finance – ISD

Overview

- Terms and Definitions
- BYOD Use
- Objective
- OIT Policy 320 – Use of POMD for State Business
- OIT Form 320F1 – User Agreement Form
- Effective and Compliance Dates
- Questions and Answers

Terms and Definitions

- **POMD** – Personally Owned Mobile Device (non-state owned)
- **Mobile Device** – Smart Phones and Tablets.
- **Centrally Managed** – Managed by the AD Forest Owner
- **Container Solution** – Software that separates state data and apps from personal
- **Non-Exempt Employee** –Employee Paid by the Hour

BYOD Use

Allowing BYOD use is not a requirement of the State, nor an employee right; but rather, a value-added accommodation made by the State and your Agency.

BYOD Use is Growing

- By 2017 one in two firms will no longer provide devices to their employees (*Gartner*)
- It is estimated that 70% of mobile professionals will conduct their work on personal smart devices by 2018 (*Gartner*)
- 90% of workers in the United States are using their personal smartphones for work purposes (*Cisco*)
- Nearly half of IT managers strongly agree that BYOD has a positive impact on the output of workers (*Intel*)
- Around 82% of companies let their staff use personal devices in the office (*Intel*)

Objective

Establish governance for the use of Personally Owned Mobile Devices (POMDs) by authorized personnel for state business, while **protecting State IT resources from corruption and unauthorized access and use.**

OIT Policy 320

Use of POMD for State Business

OFFICE OF
INFORMATION
TECHNOLOGY
STATE OF ALABAMA

Applicability and Scope

- Non-Exempt employees may only use their POMD during their normal scheduled work hours, unless prior written approval from supervisor is given
- Includes Contract staff
- Covers Mobile Devices only
- Agencies may decide to disallow use of POMDs

Applicability and Scope (cont.)

- This policy does NOT cover:
  - State-Owned Devices
  - Use of Personally-Owned PCs, Desktops, Laptops, E-Readers, etc.
  - Outlook Web Access

OFFICE OF INFORMATION TECHNOLOGY STATE OF ALABAMA

Statement of Policy

- Screen lock on the POMD must be enabled
- Use of container solution to keep State apps and data separate from personal apps and data
- Ability to remotely wipe State data from the POMD
- FIPS 140-2 compliant encryption for data in transit and at rest on the POMD

Statement of Policy (cont.)

- Data Protection Compliance
  - HIPAA
  - PHI
  - PII
  - CJI
  - FTI
  - FERPA
  - Data protected by the Code of Alabama, Alabama Administrative Code, or other written policy

Agency Responsibilities

- Container Solution must be managed and administered centrally by the State agency who manages their Active Directory Forest
- Enforce compliance of policy
- Manage implementation and maintenance of program
- Keep User Agreement Form on file until employee leaves state service, or discontinues use.

OFFICE OF INFORMATION TECHNOLOGY STATE OF ALABAMA

OIT Form 320F1
User Agreement Form

User Agreement Form

- Constitutes a directive that must be followed
- Must be signed by employee prior to using POMD
- Consequences for violation of Policy and/or Agreement Form, up to and including termination from employment
- Signature acknowledges agreement that user has read, understands, and will abide by the contents of the Form and Policy

OFFICE OF INFORMATION TECHNOLOGY STATE OF ALABAMA

Effective and Compliance Dates

- OIT Policy 320 is effective on **June 24, 2016.**
- Agencies must be in compliance by **Oct 1, 2016**.
- Posted at: http://www.oit.alabama.gov/library.aspx

Questions and Answers

Office of Information Technology

RSA Dexter Building
445 Dexter Avenue, Suite 9050
Montgomery, Al 36130
334.242.7360
Website: www.oit.alabama.gov
Email: infoOIT@oit.alabama.gov