BYOD Policy Release

Joanne E. Hale, PhD
Acting Secretary of Information Technology
Office of Information Technology

June 23, 2016
Agenda

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

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