

	Effective Date:	08-01-2016
	Policy #:	G-36
	Supersedes:	
Subject: Use of State-owned Portable Devices		Page: 1 of 5

POLICY

To provide for the management, control, and secure use of state-owned portable devices authorized for use in conducting State of Michigan (SOM) business or connecting to the state's internal computing or network resources.

STANDARDS

This standard addresses security and management concerns with the physical device itself, as well as the associated applications (Apps) and data.

DEFINITIONS

Portable Device: (as used in this document) Includes but is not limited to: laptop, iPad or similar tablet, personal digital assistant (PDA), cell phone, smartphone (e.g. Blackberry, iPhone, Droid), flash drive, and any emerging technology containing a processor and/or memory. Any device configured to send/receive SOM email; or connect to SOM internal resources or network applications.

Privately-owned: Any device that does not meet the definition of state-owned.

State-owned: Any device purchased and provided by the state and used under the provisions of an assigned contract with the state.

POLICY

Acceptable Use: All procurement and usage is governed by the [1340.00.110.05 Procurement and Use of State Wireless Devices by State Employees](#). Primary use of any SOM-owned portable device is for official State of Michigan business only. Personal use of these devices shall be limited to infrequent, incidental and/or emergency use.

	Effective Date:	08-01-2016
	Policy #:	G-36
	Supersedes:	
Subject: Use of State-owned Portable Devices		Page: 2 of 5

Authorization: Purchase requests shall be sent to LARA, Finance and Administrative Services (FAS), Office Services Division using the current [TRAD](#) request form. Purchase approval authority rests with the Director of Finance or his/her designee.

State of Michigan Licensed Software: Software (Apps) shall not be installed on state-owned devices without prior authorization and approval from LARA FAS/Office Services, or unless installed by DTMB in support of device management, security or policy enforcement. Procurement Card purchases of Apps are not allowed.

Compliance: Subject to applicable laws, regulations, and compliance requirements specific to the state business being conducted and data being handled.

Sensitive Data: Sensitive data on state-owned devices is governed by [IT 1340.00.110.03 Storage of Sensitive Information on Mobile Devices & Portable Media](#)

Physical Security: All users of these portable devices must employ reasonable physical security measures at all times.
DO NOT LEAVE YOUR DEVICE UNATTENDED!

Repair & Maintenance: Repair or maintenance must be reported and processed through LARA, FAS Office Services

	Effective Date:	08-01-2016
	Policy #:	G-36
	Supersedes:	
Subject: Use of State-owned Portable Devices		Page: 3 of 5

REQUIREMENTS SPECIFIC TO DEVICES CONFIGURED TO SEND/RECEIVE STATE OF MICHIGAN (SOM) EMAIL:

Approved Models: Only models available under current contract terms, and identified by DTMB as being supportable, shall be eligible for use by state employees.

Support Services: Technical support for state-owned devices is the device owner's responsibility. LARA, FAS Office Services support personnel will perform limited support such as provisioning setup and configuration of the device so it can receive state email. DTMB Support staff will be responsible for limited diagnostic activities to establish whether a problem might be hardware, software, security incident related, and repairs.

Email Redirection: The redirection or push of email from the state's email environment shall be state controlled via a centrally managed server. Desktop or Internet controlled email redirection, including mailbox forwarding rules – where SOM email is forwarded to a non-SOM email account, is not authorized.

DO NOT LEAVE YOUR DEVICE UNATTENDED!

Stolen Devices: Users must report any stolen device to authorities. A formal police report must be obtained and provided to LARA FAS Office Services.

Lost or Damaged: Users must contact LARA FAS Office Services. Users will be responsible for charges, including device replacement.

Precautions: Devices shall not be left unattended without employing adequate safeguards, such as restricted access or lockable cabinets.

When possible, devices shall remain under visual control while traveling. If visual control cannot be maintained, then necessary

	Effective Date:	08-01-2016
	Policy #:	G-36
	Supersedes:	
Subject: Use of State-owned Portable Devices		Page: 4 of 5

safeguards shall be employed to protect the physical device and removable components or media.

Devices shall not be left in a vehicle where they can be seen through a window and the vehicle must be locked.

DTMB Management and Policy Enforcement

Other Platforms

At a minimum, until more advanced functionality can be implemented, the following policies will be enforced:

1. User Authentication The portable device must be protected by authenticated logon using a PIN, password, or passphrase. Users shall not bypass device authentication.

2. Data Wipe The DTMB system administrator shall have the capability to remotely transmit a “data wipe” (hard reset) command to the portable device. The “Data Wipe” function will erase all data (operating system, applications, and data) stored in user addressable memory on the handheld device.

3. Password Controls Strong password controls must be implemented on the portable device. This includes setting the length of the password, the character set and password history. These will be configured according to SOM password standards.

4. Password expiration Users must change their passwords after a set period of time as determined by State of Michigan password standards.

5. Lockout after failed attempts Users will not be able to log-on to hand held devices after a set amount of failed attempts to logon. The amount of failed attempts is set by DTMB. DTMB can reset passcodes via trouble ticket.

6. Encryption The hand device and its storage cards will be encrypted.

	Effective Date:	08-01-2016
	Policy #:	G-36
	Supersedes:	
Subject: Use of State-owned Portable Devices		Page: 5 of 5

7. Inactive Time Out Users will be prompted for a password to unlock the portable device after a specific amount of time as stated in the State of Michigan standard.

Carrier Service: Financial, as well as contractual obligation for any carrier service plan (cellular, broadband) associated with the device is the sole responsibility of LARA.

All policies and procedures for Portable Devices are subject to change as deemed necessary by the department or DTMB.