STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-MDM-001	**Revision Number:** 1
Document Type:	Enterprise Policy	**Page:** 1 of 7
Policy Title:	Mobile Device Management Policy	

Synopsis:	Provide Guidance and Assurances for the Use of Mobile Device Management Software		
Authority:	Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"		
Applicability:	This Policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.		
Effective Date:	5/26/2015	**Expiration Date:**	None
POC for Changes:	Jason Clarke, Chief Operating Officer		
Approval By:	James Collins, Chief Information Officer		
Approved On:	5/26/2015		

TABLE OF CONTENTS

I. Policy

EXECUTIVE SUMMARY
This policy establishes the principles to govern the safety of State owned data when accessed by mobile devices.

PURPOSE
The purpose of this policy is to outline the management requirements and security expectations when using either personal or State owned mobile devices that access State content.

This policy covers only mobile devices.

POLICY STATEMENT

I. Any mobile device that synchronizes e-mail and/or calendars must follow the State's Mobile Device Management standard.

II. When a mobile device must access or store non-public State data (Confidential, Secret, or Top Secret data, including Federal Tax Information (FTI)) (other than email and/or calendars), it must be a State owned device, which is governed by the State's Acceptable Use Policy.

Also reference the Data Classification Policy and Data Classification Guideline.

III. Jailbroken or rooted devices will not be allowed access to the State's infrastructure.

IV. Agencies using mobile devices to access or store non-public State data must have their Mobile Device Management strategy and lost device plan vetted and approved by the Architecture Review Board prior to implementation.

This strategy must include:

A Mobile Device Management (MDM) solution that will be used to manage configuration and enforce security policies on devices.

The mobile device must be configured to use an encrypted network connection at all times when accessing non-public State data.

The mobile device user must not connect non-State controlled devices to a State mobile device.

The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.

The mobile device should only store non-public State data if approved by the agency Information Security Officer (ISO) (or designee).

Only authorized users are permitted to install software on mobile devices accessing non-public State data.

The mobile device must be configured to require all non-public State data be encrypted.

The mobile device must be configured to allow a remote wipe of all data stored on the device.

The lost or stolen mobile device should be remotely wiped within 24-hours of the incident.

The mobile device screen lock must be configured to engage after a maximum of 5 minutes of inactivity.

The mobile device must be configured to prohibit the storage of passwords in clear text.

The mobile device must be configured to prohibit reuse of previous passcodes.

The mobile device must be configured to require an expiring passcode.

The mobile device must be configured to automatically wipe the contents of the mobile device if 10 consecutive invalid login attempts occur.

V. USE OF EXTERNAL INFORMATION SYSTEMS

Note: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

1. The ISO shall permit authorized individuals to use an external information system to access the information system or to process, store, or transmit VITA-controlled information only when:

    a. The ISO can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

    b. The ISO has approved information system connection or processing agreements with the organizational entity hosting the external information system.

2. Access to network resources, including the Internet, will be via broadband or modem dial-in and Virtual Private Networking (VPN). This does not apply to users accessing Microsoft Outlook Web Access from a remote location.

3. The ISO shall limit the use of organization-controlled portable storage media by authorized individuals on external information systems.

4. Users are not allowed to use or store personal IT assets in facilities that house IT systems and data.

IMPLEMENTATION RESPONSIBILITY

DTI and/or the agency's technical staff will implement this policy during the course of normal business activities.

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This policy may also be enforced by others during the course of their normal business activities, including audits.

If there is ambiguity or confusion regarding any part of this policy, contact your supervisor or IRM.

II. Definitions

1) **Mobile Device:** A mobile device is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds. A mobile computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities. Any device that can be carried by a person and can contain digital data even temporarily. Examples of mobile devices are tablets, and Smartphones.

2) **Mobile Device Management (MDM)** – secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. MDM functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices. This applies to State -owned devices and BYOD across the enterprise. By controlling and protecting the data and configuration ~~settings~~ for mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime.

III. Development and Revision History

Initial version established **5/26/2015**
First revision established **1/25/2015**:
Added language to satisfy IRS findings regarding Mobile Device Access Controls.

IV. Signature Block

Name & Title: James Collins State Chief Information Officer	**Date**

Policies and Standards

Delaware Information Security Policy
Acceptable Use Policy
Mobile Device Management Standard