Standard ID:	**SE-SME-001**
Title:	**Mobile Device Management Standard**
Domain:	**Platform**
Discipline:	**Device Management**
Update Date: Revision no.: Original date:	**9/27/2019** **0** **5/26/2015**

I. Authority, Applicability and Purpose

A. 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"

B. Applicability: Applies to all 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, 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 and standards promulgated by DTI as a condition of funding, access, and continued use of these resources.

C. Purpose: State of Delaware Staff (State employees, contractor personnel, and casual seasonal employees) that use mobile technology to provide services to our citizens. These devices can contain sensitive data. Since this data is protected from disclosure by State and Federal laws, it is imperative that the State of Delaware secure the data entrusted to it by providing a safe and secure environment. Since mobile devices are susceptible to loss or theft, this standard sets forth the requirements for mobile security management, mobile software management, mobile content management, analytics and management delivery styles.

II. Scope

A. **All Mobile Devices** that synchronize with State e-mail, or store State non-public data. In accordance with State Security Policies and Standards, all data classified as State of Delaware Confidential, Secret or Top Secret must be protected regardless of the medium on which it is recorded. This standard pertains to mobile devices that contain classified data. Consult the State IT Policy and Standards web page for further information

B. **Environments:** This standard covers all mobile devices that synchronize with State e-mail or, retains non-Public State data. All State systems and State owned information are covered regardless of use by state employees, contractors, casual seasonal employees, or others to whom State data is entrusted. This standard covers all hand-held mobile devices such as smart phones, tablets, PDA's and phablets[1]. Only mobile devices that are compatible with the approved device management software products listed below can be used to hold State of Delaware data. This standard does not cover other environments such as desktops, servers, backup tapes, SAN storage, etc.

III. Process

A. **Adoption:** These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. **Revision:** Technology is constantly evolving; therefore, the standards will need to be regularly reviewed. It is the intent of TASC to review each standard annually. TASC is open to suggestions and comments from knowledgeable individuals within the State, although we ask that they be channeled through your Information Resource Manager (IRM).

C. **Contractors:** Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact TASC at dti_tasc@state.de.us.

D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement this standard during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. **Enforcement:** DTI will enforce this standard 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 standard may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. **Contact us:** Any questions or comments should be directed to dti_tasc@state.de.us.

[1] a smartphone having a screen which is intermediate in size between that of a typical smartphone and a tablet computer

IV. Definitions/Declarations

A. Definitions:

1) BYOD – (Bring Your Own Device): Any device that is used for State business and is not supplied by or owned by the State of Delaware.
2) 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, PDA's, Smartphones to name a few.
3) 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.[2]

B. Declarations:

1) Any personal device that is used to conduct State business must, to some degree, be managed by the State according to State specifications. Thus, the owner of that personal device must accept the management controls. Each agency will determine any additional level of control it will have over personal information.
2) In those cases where ActiveSync or containerization is not compatible with a device, operating system, or carrier, the State will require the replacement of the non-standard device with one that can meet State standards.

[2] https://en.wikipedia.org/wiki/Mobile_device_management

V. Definition of Ratings

Individual components within a Standard will be rated in one of the following categories

COMPONENT RATING	USAGE NOTES
STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and can be expected to enjoy a useful life of 3+ years from the Effective Date.	These components can be used without explicit DTI approval for both **new projects** and **enhancement** of existing systems.
DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.	Via the State's waiver process, these components must be explicitly approved by DTI for **all projects**. They must not be used for **minor enhancement** and **system maintenance** without explicit DTI approval via the State's waiver process.
DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	No waiver requests for new solutions with this component rating will be considered.

A. **Missing Components** – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information.

VI. Component Assessments

A. The State requires that all mobile devices that synchronize with State e-mail or hold State data will be managed equipped with one of the named Component Products listed below as per the Mobile Device Management Policy.

B. The State will not require State organizations to use a centralized key management solution for mobile devices. Individual State organizations should develop plans for key recovery prior to implementation.

#	Component	Rating	Comments
1	AirWatch http://www.air-watch.com/	Standard	Utilize AirWatch when holding State non-public data on State owned mobile devices.[3] AirWatch is not required, when ActiveSync is managing the data.
2	ActiveSync	Standard	For synchronizing e-mail, on personal and State owned mobile devices.

[3] Data Classification Policy