Standard ID:	**SE-SME-001**
Title:	**Mobile Device Encryption Standard**
Domain:	**Security**
Discipline:	**Data Security**
Update Date: Revision no.: Original date:	**05/30/2017** **7** **2/4/2008**

I. Authority, Applicability and Purpose

A. **Authority:** Title 29, Chapter 90C provides broad statutory authority to the Department of Technology and Information to implement statewide and interagency technology solutions, policy, standards, and guidelines for the State of Delaware's technology infrastructure. "Technology" means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information or data electronically. Technology also includes systems and equipment associated with e-government and Internet initiatives.

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) 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 acceptable methods to encrypt and protect data on mobile devices. In some cases, the device itself may need to be recovered. As such, it is important that the State be able to recover the data on mobile device if for any reason, the encryption key is forgotten, lost, or unavailable.

II. Scope

A. **Mobile Devices Containing Sensitive State Information:** In accordance with State Security Policies and Standards[1], 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.

B. **Environments:** This standard covers all mobile devices that contain classified information regardless of use by state employees, contractors, casual seasonal employees, or others to whom State data is entrusted. This standard covers laptops, USB storage devices, tablet PCs, and removable media. Only mobile devices that are compatible with State standards may be used for the storage of State data if it is classified other than Public. Only mobile devices that are State network attachable and are compatible with the approved products can be used to hold State of Delaware Confidential, Secret, or Top-Secret data. This standard does not cover other 'data at rest' environments such as desktops, servers, backup tapes, SAN storage, PDA's 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] http://dti.delaware.gov/information/standards-policies.shtml

IV. Definitions/Declarations

A. Definitions:

1) Encryption: Encoding data so that an unauthorized party cannot decipher or alter it.
2) Full Disk Encryption: It uses disk encryption software or hardware to encrypt every bit of data that goes on disk or disk volume.[2]
3) Mobile Device: Any device that can be carried by a person and can contain digital data even temporarily. Examples of mobile devices are laptops, tablet PCs, USB memory and USB drives.
4) Pre-boot authentication: It prevents anything being read from the hard disk such as the operating system until the user has confirmed he/she has the correct password or other credentials.[3]
5) Removable Media: Refers to storage media, which can be removed from its reader device, conferring portability on the data it carries. Examples include CD-ROMs, DVD-Rs, Zip disks.

B. Declarations:

1) If a mobile device is to use encryption, it must use full disk encryption, if further encryption is required for folders or files, they may be further encrypted.
2) If a device cannot utilize full disk encryption because of its file system, operating system, age, applications, etc. the device should be restricted to Public Data only.
3) Before full deployment, encryption packages and their options should be tested thoroughly to ensure compatibility with application software and data.

[2] http://en.wikipedia.org/wiki/Full_disk_encryption

[3] http://en.wikipedia.org/wiki/Pre-boot_authentication

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 solidly positioned in its product life cycle.	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. All of these products have not yet been tested or proven to work in the State's environment. If one of these products is to be chosen, coordination with your organization's IRM and DTI prior to selection must occur.

B. DTI 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.

C. It is recommended that organizations use the encryption capabilities of the below components to protect removable media and USB devices, which contain copies or backups of State of Delaware confidential, secret or top secret data.

#	Component	Rating	Comments
1	BitLocker	Standard	Native component of Microsoft Windows 7 Ultimate and Enterprise products. Not available for other platforms. In FIPS mode, many useful features are switched off; however, in non-FIPS mode, BitLocker is vulnerable to recovery key access by Active Directory administrators. BitLocker To Go is limited to read-only access on Vista and XP, and cannot be read on other platforms.
2	PointSec	Standard	Formerly Check Point Can only be used within a VRF - uses File Share to communicate between the policy server and the encrypted devices.
3	Sophos SafeGuard	Standard	Formerly Utimaco
4	Trend Micro Endpoint Encryption	Declining	(Licensed by Credent, SanDisk, and IronKey)
5	McAfee Endpoint Encryption, McAfee Encrypted USB	Declining	Formerly Safeboot products
6	Symantec (GuardianEdge)	Declining	
7	WinMagic	Declining	(enhanced integration with Intel AT)