

1315.00 Policy for Storage of Sensitive Information on Mobile Devices and Portable Media

Issued June 16, 2006

SUBJECT: Policy for Storage of Sensitive Information on Mobile Devices and Portable Media

APPLICATION: Executive Branch Departments and Sub-units, private partners and contractors.

PURPOSE: To establish a statewide policy for the protection of State of Michigan (SOM) sensitive information and data stored on mobile devices and portable media.

The public rightly assumes and should be assured that the data in the possession of Michigan state government is secure and protected from unauthorized disclosure or misuse.

CONTACT AGENCY: Department of Technology, Management and Budget (DTMB)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: Any user who has been authorized to access State of Michigan sensitive information has an obligation to safeguard and protect the confidentiality of such data. The objective of this procedure is to minimize the likelihood that sensitive or confidential SOM information is inadvertently disclosed.

PROCEDURE:

- Storage of sensitive information on mobile devices or portable media is permitted only if **all** of the following requirements have been satisfied:
 - Use is restricted to individuals whose job duties require it;
 - Granted for a finite duration as needed to fulfill the specific functions required to perform a specific job;
 - Approval has been obtained by both the employee's department head (or their designee) and the system/data owner. For non-SOM employees, "department" is defined as the SOM Agency contracting with the 3rd party;
 - Sensitive data has been encrypted. Encryption must comply with DTMB Standard 1315.10 as published (http://www.michigan.gov/documents/1315_162702_7.10_Encryption_Policy.pdf). **Unencrypted storage of sensitive information on mobile devices and portable media is prohibited.** Please note that SOM Administrative Guide Procedure 1350.90 for data sanitation and media disposal will need to be followed.

- ANY instance of SOM sensitive information (*including that stored on a mobile device or portable media - encrypted or unencrypted*) being lost, stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, **must be reported immediately** to your appropriate Agency management and the Department of Technology, Management and Budget's Customer Service Center (DTMB CSC) at (517) 241-9700 or (800) 968-2644.

Terms and Definitions

Term	Definition
Data/system owner	Senior management of the Agency that is ultimately responsible for ensuring the protection and appropriate use of their business' data.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key that enables you to decrypt it.
Term	Definition
Mobile devices	<p>Any mobile device (State-owned or privately-owned) capable of storing data. Examples include, but are not limited to, laptop and tablet PCs, Blackberrys, cell phones, PDAs, iPods (MP3 players).</p> <p>For the purpose of this policy, all non-state-owned computing or data storage equipment (e.g., PC, server, NAS, SAN) are considered mobile devices.</p>
Portable media	<p>Any portable media (State-owned or privately-owned) capable of storing data.</p> <p>Examples include, but are not limited to, external hard drives, USB thumb drives, flash drives, memory sticks and cards, CDs, DVDs, floppy disks.</p>
Sensitive information and data	<p>Those data elements that are governed or restricted in some manner by a federal or state statute, rule, policy or requirement.</p> <p><u>At a minimum, sensitive information that all Agencies must encrypt includes</u> (but is not limited to):</p> <ul style="list-style-type: none"> ▪ Name and social security number pair ▪ Name and credit card number pair ▪ Personal health records as identified by HIPPA <p>In addition to above, Agencies may assign data classifications to their data elements. Encryption would be required for any Agency-specific information labeled as sensitive.</p>

- **Authority**

E.R.O. No. 2001-1, compiled at § 18.41 of the Michigan Compiled Laws (Technology, Management and Budget Act 431 of 1984: Section 18, and Executive Reorganization Order 2001-1 now contained in the Act Section 18.41 Paragraph H).

- **Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law.

Any 3rd party found to have violated this policy may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

- **Exceptions**
Exceptions to this policy may be granted solely by the Director of the Department of Technology, Management and Budget (or the Director's designee).
- **Effective Date**
Immediate upon release.

* * *