

	<i>State of Michigan Department of Technology, Management & Budget</i>	TECHNICAL STANDARD
Subject:	Electronic Data Encryption (former Ad Guide 1315.10)	Standard Number
Authoritative Policy:	<u>1340 IT Information Security Policy</u>	1340.00.07
Associated Procedures:	n/a	
Distribution:	Statewide	

Purpose: Encryption is used to provide a high level of security to the state’s electronic data by translating data into secret code. This policy identifies the requirements for encryption methods when data is transmitted in-flight or when data is stored in permanent or removable electronic media.

Contact/Owner: DTMB CyberSecurity and Infrastructure Protection (CIP)
Michigan Cyber Security (MCS)

Scope: Executive Branch Departments, Agencies, Boards or Commissions, private partners, and contractors. Any electronic device that has been authorized to access state of Michigan (SOM) sensitive information must protect the confidentiality of such data. In order to maintain a high level of security of the state’s information technology managed resources and data this standard defines a requirement to use a method of encryption both when data is in transit across internal or external networks and when stored in permanent or removable media.

Standard: Encryption must be utilized when moving or storing protected information including citizen privacy information or personally identifying information (PII) such as social security numbers, regulated health information, financial data including credit card numbers or Federal Tax Information (FTI). Through encryption methods the objective is to minimize the likelihood that sensitive or confidential SOM information is inadvertently disclosed or accessed during the transmission or storage of sensitive and/or confidential data.

1. Asymmetric Keys:
 - Keys: RSA or DSA
 - Size: 2048bit through 4096bit
2. Symmetric Keys:
 - Keys: AES or TDEA (3DES)
 - Size: Minimum 128bit, 192bit or 256bit for highly sensitive data
3. Hash Algorithm
 - SHA-1 through SHA-512

Issued: 4/28/2012
Revised: 10/30/2013
Reviewed:
Next Review Date: (1 yr) 10/30/2014

4. SOM requirements for data storage encryption:
 - Whenever supported by the underlying product suites, Transparent Data Encryption (TDE) should be used. TDE is based on a dual encryption method that uses a secondary encryption key that is stored in a file external to the encrypted database file.
5. All SOM resources must utilize centrally managed digital certificates.
6. DTMB reviews this standard yearly.
7. Passwords which are used to generate keys, must be unique during initial implementation or regenerating new keys when they expire or are revoked.

Any employee found to have violated this standard might 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 standard might 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 standard must follow the [1305.00.02 Technical Policy and Product Exception Standard](#).

Approving Authority:

John Nixon, CPA
Director

Revised: 10/30/2013

**Issued: 4/28/2012
Revised: 10/30/2013
Reviewed:
Next Review Date: (1 yr) 10/30/2014**