STATE OF ALABAMA

Information Technology Policy

POLICY 683-00: ENCRYPTION

Encryption is a technique used to help protect the confidentiality of stored or transmitted information. As required in this and other State policies, encryption must be utilized to protect sensitive and confidential information, particularly on systems that can be transported outside protected work spaces and on communications channels that span untrusted networks. This policy addresses encryption utilization requirements, encryption methods and key length requirements.

OBJECTIVE:

Define the minimum requirements for the selection, application, and management of encryption technologies.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

- Use encryption, as specified in this policy and other applicable standards, to protect sensitive and confidential systems and information and when other controls do not provide adequate protection.
- Utilize full-disk encryption (FDE) on laptops, notebooks, netbooks, tablet PCs, and similar portable devices.
- Encrypt sensitive and confidential data on portable data storage devices (PDA, flash drive, CD, DVD, or any other external storage device) whenever technically possible.
- Define in system security plans and operating procedures key management procedures that specify key generation, storage, distribution, rotation, recovery, and zeroization.

ADDITIONAL REQUIREMENTS:

Encryption Methods:

State encryption technologies shall use proven industry standard algorithms. The use of proprietary encryption algorithms, an algorithm that has not been made public and/or has not withstood public scrutiny (regardless of whether the developer of the algorithm is a vendor, an individual, or the government) is not allowed for any purpose.

Encryption products used shall be listed on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation List (http://csrc.nist.gov/groups/STM/cmvp/validation.html) and be validated to the current Federal Information Processing Standard (FIPS).

Acceptable Methods:

Encryption methods that utilize either the Triple Data Encryption Standard (Triple DES) or the Advanced Encryption Standard (AES) are acceptable. Encryption methods shown below can also be used to protect sensitive and confidential information:

- Virtual Private Network (VPN) – allows information to be sent securely between two end stations or networks over an un-trusted communications medium; use of VPN technology is the preferred method for securing sensitive and confidential communications.

- IPSEC – is suitable for all types of Internet Protocol (IP) traffic, and may be used to secure Internet and other IP communications within State and agency networks and to connect to authorized external customers.
- Secure Sockets Layer (SSL) – may be deployed to provide secured access to sensitive and confidential information on Web servers.
- Secure Shell (SSH) – may be utilized for the remote administration of sensitive systems.
- Approved Hash Algorithms: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. (SHA-1 may not be suitable for digital signature application requiring greater than 80-bit security unless using the randomized hashing technique described in NIST Special Publication 800-106). Other hashing methods, some in wide-spread use such as MD5, are not recommended.

Other methods of encryption require explicit approval of the State IT Security Council before being used to protect State data or systems.

Unacceptable Methods:

Unacceptable methods of encryption include:

- Data Encryption Standard (DES)
- Wired Equivalent Privacy (WEP)

Key Length:

Symmetric cryptosystems (such as AES) require a minimum 128-bit key length.

Asymmetric cryptosystems (such as RSA) require key lengths equivalent to a 128 bit or longer symmetric key. Example: A 3072-bit RSA key is equivalent to a 128-bit symmetric key.

SUPPORTING DOCUMENTS:

- Information Technology Standard 681S1: Information Protection

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
683-00	09/01/2011	Replaces Policy 680-03 and Standard 680-03S1; number and format change only