



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 683S1: Encryption Requirements

VERSION NUMBER	Standard 683S1-01
VERSION DATE	July 30, 2019
STANDARD TITLE	Encryption Requirements
GOVERNING POLICY	This standard is governed by Policy 683: Encryption, regardless of revision.
OBJECTIVE	To ensure information systems protect the confidentiality and integrity of information as it transmitted to or from the state enterprise network, whether transferred between state agencies or with external entities, and while at rest, residing on state-owned information systems.
REQUIREMENTS	<ol style="list-style-type: none">1. CRYPTOGRAPHIC PROTECTION - GENERAL<ol style="list-style-type: none">1.1. Where encryption is required and used within an information system, the cryptographic implementation shall use Federal Information Processing Standard (FIPS) validated cryptography or National Security Agency (NSA) approved cryptography. [SC-13]1.2. Cryptographic modules shall be implemented in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. [SC-13]1.3. Acceptable Methods of Encryption:<ol style="list-style-type: none">1.3.1. Encryption methods that utilize the Advanced Encryption Standard (AES) are acceptable. Additional, encryption methods listed below may also be used to protect sensitive and confidential information:<ul style="list-style-type: none">• Virtual Private Network (VPN)• IPSEC• Secure Shell (SSH)• TLS (Transport Layer Security) 1.2 or higher• Secure Hash Algorithms (SHA): SHA-2, SHA-3, SHA-224, SHA-256, SHA-384 and SHA-512

1.3.2. Use encryption products that are validated to the current FIPS standards and are listed on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation List:
(<http://csrc.nist.gov/groups/STM/cmvp/validation.html>).

1.4. Non-Acceptable Methods of Encryption: Encryption algorithms with documented occurrences of compromise shall not be authorized for use on state owned information systems or networks. These unapproved encryption methods are:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (TDES or 3DES)
- Wired Equivalent Privacy (WEP)
- Message-Digest Algorithm (MD5)
- SHA-1
- TLS 1.0 and 1.1

1.5. Cryptographic Key Management:

1.5.1. Agencies that manage cryptographic keys shall implement procedures compliant with Federal Information Processing Standard (FIPS) key management processes for key generation, distribution, storage, access, and destruction. [SC-12]

1.5.2. Agencies shall issue public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider. [SC-17]

1.5.3. Agencies shall define procedures addressing public key infrastructure certificates, public key certificate policies, and public key issuing processes. [SC-17]

1.5.4. Agencies shall define in system security plans or operating procedures key management procedures that specify key generation, storage, distribution, rotation, recovery, and zeroization.

1.5.5. 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.

2. DATA AT REST

2.1. Agencies shall configure information systems, mobile devices, and portable storage devices to protect the confidentiality and integrity of sensitive data (e.g., federal tax information (FTI)) when that data resides on information system primary storage or on a portable storage device. [SC-28]

2.2. Where at-rest data encryption is required, agencies may choose whether to encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). [SC-28 (CE1)]

3. FILE TRANSFER

3.1. File transfer protocol (FTP) shall utilize an encryption methodology such as Secure Shell (SSH) to prevent unauthorized disclosure or modification of sensitive or confidential information during transmission of files to or from systems external to the state-controlled network. [SC-8]

3.2. Agency information systems shall be configured to utilize only authorized software and secure methods to execute secure file transfers via FTP/SFTP. [SC-8]

3.3. Coordination between agencies or external entities exchanging information shall be accomplished prior to transmission to ensure file transfers are secure.

4. EMAIL

4.1. Personnel transferring sensitive or confidential information via email shall utilize message encryption.

4.2. To enable email message encryption in Office 365, insert “[ENCRYPT]” in the subject line of the message.

4.2.1. [ENCRYPT] may not be required if the Office 365 tenant is enforcing encryption of specific sensitive data types.

4.2.2. The OIT Office 365 tenant shall automatically enforce encryption of:

- US Social Security Number
- US Individual Tax Identification Number
- US Passport Number
- US Bank Account Number
- Credit Card Number

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 683: Encryption](#)

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support these requirements and may aid in their implementation:

- NIST SP 800-53R4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- FIPS Publication 140-2: Security Requirements for Cryptographic Modules

EFFECTIVE DATE This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES This is the initial standard and does not supersede a previous version.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the _____ day of _____, 2019.

Marty Redden
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
683S1-01	07/30/2019	Initial version