

# **DRAFT Standard Statement – Encryption**

**Title:** Encryption Standard

**Document Number:** SS-70-006

**Effective Date:** xx/xx/2011

**Published by:** Department of Information Systems

## **1. Purpose**

Sensitive information held by public organizations can include social security numbers, credit card numbers, and other personal information about Arkansas' citizens. Government, in particular, is responsible for information that protects public health and public safety. Individuals with malicious intent can easily acquire information being transmitted electronically unless appropriate security measures are applied, such as encryption.

If detected, the credentials employees use to access data and systems can provide unauthorized access which can lead to critical data being modified, deleted and ultimately made unavailable. For these reasons very sensitive information must be protected through encryption methods.

## **2. Scope**

This standard statement applies to all state agencies, boards, commissions, and administrative sections of institutions of higher education.

## **3. Background**

Arkansas Code Ann. Section 25-4-105(13) and (15)(Supp. 2007) gives the Department of Information Systems the authority to define standards, policies and specifications for state agencies and ensuring agencies' compliance with those policies, procedures and standards. In addition, the department develops information technology security policy for state agencies.

The State Security Working Group, made up of representatives of state agencies and higher education, wrote the Encryption Standard.

## **4. References**

- 4.1** Data and System Security Classification Standard (SS-70-001)
- 4.2** Physical and Logical Security Standard (SS-70-008)
- 4.3** Wireless Security Standard (SS-70-010)

## 5. Standard

- 5.1** The following standard applies only to data that is classified by the SS-70-001 [Data and System Security Classification Standard](#) as being Level C - Very Sensitive or Level D - Extremely Sensitive and transmitted on a public network, including the State Network, or removed from a covered entity's physical location.
- 5.1.1** Users accessing data from outside organizational local area networks shall encrypt their credentials, including login IDs and passwords, to access such data.
  - 5.1.2** Data on all portable media and mobile computing devices, such as laptops, PDAs, flash drives, CDs, DVDs, or any external storage device shall be encrypted.
  - 5.1.3** Backups for business continuity purposes that are taken offsite shall be encrypted.
    - 5.1.3.1** Archived backups created prior to the effective date of this standard are exempt from this encryption requirement and are subject to the requirements of the Physical and Logical Security Standard (SS-70-008).
    - 5.1.3.2** Encryption keys used to encrypt data used for business continuity purposes must be stored offsite within a locked or otherwise restricted environment in a building. Data shall be encrypted with algorithms utilizing 128 bit encryption, at a minimum.
  - 5.1.4** 5.1.4 Encryption products used shall be listed in the NIST cryptographic module validation list and validated to the current FIPS standard. Acceptable methods of 128 bit or higher encryption include, but are not limited to:
    - 5.1.4.1** Triple-DES
    - 5.1.4.2** Advanced Encryption Standard
    - 5.1.4.3** International Data Encryption Algorithm (IDEA)
    - 5.1.4.4** RSA (key length must be 1024 bits or higher)
    - 5.1.4.5** SSL/TLS (secure socket layer)
    - 5.1.4.6** Blowfish
    - 5.1.4.7** ElGamal
    - 5.1.4.8** SHA-2 (definition)
  - 5.1.5** Unacceptable encryption methods include, *but are not limited to*:
    - 5.1.5.1** DES (Data Encryption Standard)
    - 5.1.5.2** MD5 (Message-Digest algorithm 5)
  - 5.1.6** Encryption shall be used for data transmissions such as FTP (file transfer protocol) and Telnet. Methods of acceptable encryption include, but are not limited to, SSH, third party secure FTP solutions, and the use of a secure virtual private network (VPN).

5.1.7 All email servers must be configured to accept TLS as the preferred connection method.

## 6. Procedures

The State Cyber Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Cyber Security Office has the right to grant an exception or exclusion to any part of this standard. The Arkansas Division of Legislative Audit also audits for compliance with this standard.

## 7. Revision History

Date	Description of Change
x/x/2010	Original Standard Statement Published

## 8. Definitions

### 8.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is an encryption algorithm utilizing the Rijndael specification for securing information by federal government agencies. Key sizes of 128, 192, and 256 bits are specified in the AES standard. AES was approved by the National Institute of Standards and Technology (NIST) as US FIPS PUB 197.

### 8.2 Backup

Information archived for the purpose of recovering systems and data in the event of a disaster or loss of data.

### 8.3 Data Encryption Standard (DES)

The Data Encryption Standard is a symmetric key algorithm adopted by the federal government as a federal standard for protecting sensitive unclassified information. With an effective key length of 56 bits, DES was compromised in 1997.

### 8.4 File Transfer Protocol (FTP)

An application layer protocol used to transfer bulk-data files between machines or hosts according to RFC959.

### 8.5 Flash drive

Flash drives, also referred to as thumb drives or USB drives, are portable storage devices that use flash memory and are very lightweight and small. Flash drives can be used in place of a floppy disk, zip drive disk, or CD.

### 8.6 MD5 (Message-Digest algorithm 5)

Designed by Ronald Rivest, MD5 is a cryptographic hash function that creates a 128-bit hash or representation of a message to provide data integrity. MD5 is not resistant

to collision or the ability for two different hashes to represent the same message. As a result, MD5 should not be used for digital certificates or SSL applications.

### **8.7 RSA**

The RSA algorithm, developed by Rivest, Shamir and Adleman, can be used for public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

### **8.8 Secure Shell (SSH)**

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. Both ends of the client/server connection are authenticated using a digital certificate and passwords are encrypted. SSH uses RSA public key cryptography for both connection and authentication. SSH-1 is considered obsolete as it is susceptible to man-in-the-middle attacks. SSH-2 replaces SSH-1.

### **8.9 Secure Socket Layer/Transport Layer Security (SSL/TLS)**

SSL/TLS is a protocol uses the public-and-private key encryption system, which also includes the use of a digital certificate. SSL/TLS is an integral part of most Web browsers (clients) and Web servers.

### **8.10 State Network**

The State network means the shared portions of the state's telecommunications transmission facilities, including all transmission lines and all associated equipment and software components necessary for the management and control of the state network. The state network is the backbone and doesn't include the local area networks.

### **8.11 Telnet**

Telnet is a network protocol that is used to connect to remote computers for the purpose of executing commands on a remote machine. Telnet is considered to be insecure due to several well-known vulnerabilities.

### **8.12 Triple DES Encryption**

Triple DES encryption encrypts data using the DES algorithm three times. Three 56-bit keys are used, instead of one, for an overall key length of 192 bits.

### **8.13 Secure Virtual Private Network (VPN)**

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

## **9. Related Resources**

**9.1** COBIT standards: [www.isaca.org/cobit.htm](http://www.isaca.org/cobit.htm)

- 9.2 Act 1526 of 2005: <ftp://www.arkleg.state.ar.us/acts/2005/public/Act1526.pdf>
- 9.3 HIPAA Security Standards: <http://www.hipaadvisory.com/regs/finalsecurity/>
- 9.4 NIST Advanced Encryption Standard: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- 9.5 FIPS (Federal Information Processing Standards) Module Validation Lists:  
<http://csrc.nist.gov/groups/STM/cmvp/validation.html>
- 9.6 American Reinvestment and Recovery Act HITECH (Health Information Technology for Economic and Clinical Health ) Act Breach Notification Rule:  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>
- 9.7 RFC959.org: <http://tools.ietf.org/html/rfc959>

## 10. Inquiries

Direct inquiries about this standard to:

Department of Information Systems  
State Cyber Security Office  
One Capitol Mall  
Little Rock, Arkansas 72201  
Phone: 501-682-2701  
FAX: 501-682-4310  
Email: [itpolicyteam@arkansas.gov](mailto:itpolicyteam@arkansas.gov)

DIS standards, policies and best practices can be found on the Internet at:  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>