Appalachian STATE UNIVERSITY

Encryption Standard

Revision Notes: Version 1.0 - 5/2016	Last Updated: 05/2016	Status: DRAFT

Table of Contents

1. Objective:

The objective of this standard is to clearly define the requirements necessary for securely managing encryption technologies in order to provide acceptable levels of protection for institutional data and systems.

2. Scope:

The standard applies to all Appalachian State University employees, students, and affiliates and all institutional systems and data (see section 4.4) whether individually controlled, shared, stand alone, or networked.

3. Requirements

3.1 Use Of Secure Ciphers + Cryptographic Protocols

University owned systems must not utilize known weak encryption methods or components including, but not limited to, encryption ciphers, network cryptographic protocols, wireless encryption methods and cryptographic hash functions.

3.1.1 Disallowed Weak Encryption Ciphers

The following encryption ciphers are known to have security issues should not be used on Appalachian State University systems. If one of these methods are employed, then this must be changed (see section 3.1.3 for recommended methods).

- Disallowed Network Cryptographic Protocols: RC4, SSL (all vers), TLS v1.0
- Disallowed Weak Wireless Encryption Protocols: WEP, WPA

3.1.2 Disallowed Data Obfuscation and Proprietary Encryption Methods

Data Obfuscation methods are not to be used as substitute for actual encryption (e.g. XOR).

Proprietary encryption methods are not to be used; Encryption ciphers and methods should have open to public scrutiny including the cryptography research community.

3.1.3 Recommended Ciphers + Cryptographic Protocols

The following ciphers and cryptographic protocols are recommended for use on University systems.

- Recommended Network Cryptographic Protocols: TLS 1.1+, Kerberos, IPSEC
(Note cryptographic protocol must also employ approved ciphers below.)

- Recommended Data Encryption Ciphers: AES, TwoFish, Serpent, Blowfish, TripleDES
(Note: Note key length should exceed 112 bits. See 3.1.4)
- Recommended Cryptographic Hash Functions: SHA2, SHA3,

3.2 Key Management

3.1.1 Key Recovery, Escrow, and Data Recovery

All information that is encrypted on University-owned systems, devices, or media must be recoverable by the University departmental staff or by authorized ITS employees. Encryption keys used to encrypt data must be securely backed-up by unit and/or held in escrow by ITS Office of Information Security.

3.1.2 Key Backups and Protection

Encryption keys should be treated as confidential data and access to these keys should be limited to only those with a legitimate university need to access.

3.1.4 Recommended Security Strength of Keys

Encryption keys should provide at least 112-bits of security strength.

3.1.5 Public Key Certificate Management

- **3.1.5.1 -** University technology services may not utilize self-signed certificates in production environments unless formally approved by the ITS Office of Information Security.
- **3.1.5.2 -** Signed certificates must utilize certificate authorities that have been approved by the ITS Office of Information.
- **3.1.5.3** - Wildcard certificates for APPSTATE.EDU are not permitted for services that transmit confidential or sensitive data (see data management standard).
- **3.1.5.4** - The ITS Office of Information Security maintains the authority to require the revocation of certificates when deemed necessary to minimize risks.

4.0 Enforcement, Exemptions, and Advisement

3.4.1 Authority and Enforceability - This standard is established under the authority of the Chief Information Security Officer (Information Security Policy 4.3.3). In the event of violation of this standard, the Chief Information Security Officer may require that non-compliant University IT services be disconnected or temporarily suspended until the requirements defined above are established and/or verified.

3.4.2 Exemptions - Exemptions to this standard must be undergo a formal risk evaluation and receive signed approval by the University Chief Information Officer.

3.4.3 Review and Advisement - Collaborative advisement concerning these standards are provided by the University IT Security Liaisons Group and Campus Information Security Advisory Committee.

5. Definitions

5.1 "Encryption" - encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

5.2 "Institutional system" - An Institutional System is any information system (i.e. desktop, server, mobile device) that is utilized to conduct business on the behalf of the University.

5.3 "Institutional Data" - Institutional data refers to one or more data elements that meets one or more of the following criteria:

- Any Data that originates in an academic or administrative system.
- Any Data contained within the University data warehouse.

5.4 "Cipher" - a cipher (or cypher) is an algorithm for performing encryption or decryption of data or information.

5.5 "Key Strength" - A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. (NIST 800-57).

5.6 - Wildcard Certificate - Public key certificate which can be used with multiple subdomains of a domain.

5. REFERENCES

5.1 University Information Security Policy (Key Control Requirements 4.4.3.1, 4.4.3.2)

5.2 University Statement of Confidentiality

5.3 University Identity Theft Prevention Plan

5.4 University Payment Card Services Policy

5.5 NIST 800-57 - Recommendations For Key Management