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 and should not be used on Appalachian State University systems. Any of the following ciphers should be replaced as soon as reasonably feasible by one of the recommended ciphers set forth in section 3.1.3. Note: this list will change over time as issues are discovered.

- Disallowed Network Cryptographic Protocols:
  - SSL/TLS: (All versions of SSL-Secure Sockets Layer)
  - SSL v1 (insecure)
■ SSL v2 (insecure)
■ SSL v3 (insecure)
■ TLS v1.0 (insecure)
  ○ Disallowed Cryptographic Primitives
    ■ RC4
    ■ Null Encryption, ie no encryption
    ■ Any cipher suite with 40 or 56 bit key length
  ● Disallowed Weak Wireless Encryption Protocols:
    ○ WEP
    ○ WPA
  ● Disallowed Hashing Algorithms
    ○ MD5
    ○ SHA1

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 be 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 1.2+, 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,
  ● The following cipher suite is a starting point for web services, ie https:
    ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    ○TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
    ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
    ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256
    ○ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    ○ TLS_DHE_RSA_WITH_AES_128_GCM_SHA384
    ○ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
3.2 Key Management

3.2.1 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.

3.2.2 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.

3.2.3 Recommended Security Strength of Keys
Encryption keys should provide at least 112-bits of security strength.

3.2.4 Public Key Certificate Management
- 3.2.4.1 - University technology services should not utilize self-signed certificates in production environments unless formally approved by the ITS Office of Information Security.
- 3.2.4.2 - Signed certificates must utilize certificate authorities that have been approved by the ITS Office of Information Security. Approved internal certificate authorities may only be used for internal campus services (not public-facing).
- 3.2.4.3 - Wildcard certificates for APPSTATE.EDU must not be used for Medium or High Impact Services services that transmit confidential or sensitive data (see data management standard and minimum security standard) unless formally approved by the ITS Office of Information Security.
- 3.2.4.4 - The lifespan of wildcard certificates must not exceed 1 year and must be re-keyed at renewal. The lifespan of other certificates must not exceed a 3 year lifespan unless formally approved by the ITS Office of Information Security.
- 3.2.4.5- 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

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

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

4.3 Review and Advisement - Collaborative advisement concerning these standards is provided by the University IT Implementation Group, IT Security Liaisons Group, Information Security Advisory Committee, and IT Board of Directors.

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.

6. REFERENCES

6.1 University Information Security Policy (Key Control Requirements 4.4.5.1, 4.4.5.2)

6.2 University Statement of Confidentiality

6.3 University Identity Theft Prevention Plan

6.4 University Payment Card Services Policy

6.5 NIST 800-57 - Recommendations For Key Management