State of Ohio IT Standard	
Standard Number: **ITS-SEC-01**	**Title:** **Data Encryption and Cryptography**
Effective Date: 03/12/2021	**Issued By:** Ervan D. Rodgers II, Assistant Director/State Chief Information Officer Office of Information Technology Ohio Department of Administrative Services
Version Identifier: 2.0	**Published By:** Investment and Governance Division Ohio Office of Information Technology

1.0 Purpose

This state IT standard defines the minimum requirements for ***cryptographic algorithms*** that are ***cryptographically strong*** and are used in ***security services*** that protect at-risk or ***sensitive data*** as defined and required by agency or State policy, standard or rule. This standard does not classify data elements; does not define the security schemes and mechanisms for devices such as tape backup systems, storage systems, mobile computers or removable media; and does not identify or approve secure transmission protocols that may be used to implement security requirements.

2.0 Scope

Pursuant to Ohio Administrative Policy IT-01, "Authority of the State Chief Information Officer to Establish Ohio IT Policy," this state IT standard is applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.

3.0 Background

The ***National Institute of Standards and Technology*** (***NIST***) conducts extensive research and development in cryptography techniques. Their publications include technical standards for data encryption, digital signature and message authentication as well as guidelines for implementing information security and managing cryptographic keys. These standards and guidelines have been mandated for use in federal agencies and adopted by state governments and private enterprises.

This state IT standard adopts a subset of the NIST standards and guidelines for implementing cryptographically strong information security for the State of Ohio.

4.0 Standard

A security service conforming to this state IT standard embeds validated ***cryptographic modules*** (see section 4.1) and uses approved cryptographic algorithms (see section 4.2) in its implementation. Furthermore, the description of the cryptographic implementation shall be kept confidential (see section 4.3). Any use of cryptographic modules for electronic signatures must also comply with rule 123:3-1-01 of the Ohio Administrative Code.

4.1 Approved Cryptographic Modules

4.1.1 Validated Cryptographic Modules

Cryptographic modules embedded in security services validated under the ***Cryptographic Module Validation Program*** (***CMVP***) in accordance with NIST Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," are approved for use through September 21, 2026. After September 21, 2026, the remaining FIPS 140-2 certificates will be moved to the historical list.

NIST FIPS Publication 140-3, "Security Requirements for Cryptographic Modules," is approved for use. Cryptographic module validations must be evidenced by a NIST-issued certificate number.

4.1.2 In Process List of Cryptographic Modules

Cryptographic modules that are on the CMVP In Process List (refer to Section 7.0 Related Resources - NIST Cryptographic Module Validation Program (CMVP) Program) are approved for use by this standard, except when such deployment may be further limited or prohibited by agency or State policy, standard or rule. Submission for testing is not a guarantee of eventual validation and, consequently, may pose a security risk. Agencies should be deliberate in determining whether their use of an unvalidated cryptographic module is appropriate. If a cryptographic module that is in use is subsequently removed from the CMVP In Process List without a certificate, continued use of the cryptographic module must cease immediately.

4.2 Approved Cryptographic Algorithms

The specification of a cryptographically strong algorithm includes the name of the approved algorithm and key length, a reference to its formal specification in a FIPS or NIST recommendation, and its acceptable use, which means that the algorithm and key length is safe to use and currently has no known security risk.

4.2.1 Symmetric Key Ciphers for Data Encryption

Cryptographic modules that use a ***symmetric key cipher*** (also referred to as private key encryption) employing a shared secret key must adhere to the specifications in Table 4-1.

Table 4-1. Approval Status of Symmetric Algorithms Used for Encryption and Decryption

Algorithm Reference	Use
Advanced Encryption Standard (AES)-128, AES-192, and AES-256 Encryption and Decryption NIST FIPS Publication 197, "Advanced Encryption Standard (AES)," November 2001.	Acceptable

4.2.2 Asymmetric Key Ciphers for Digital Signatures

Cryptographic modules that use ***asymmetric key ciphers*** (also known as public key encryption) that employ a pair of cryptographic keys consisting of one public key and one private key must adhere to the specifications in Table 4-2.

Table 4-2. Approval Status of Algorithms Used for Signature Generation and Verification

Algorithm Reference	Use
Digital Signature Algorithm (DSA): len(p) ≥ 2048 and len(q) ≥ 224 NIST FIPS PUB 186-4, "Digital Signature Standard (DSS)," July 2013.	Acceptable
Rivest, Shamir and Adleman (RSA): len(n) ≥ 2048 NIST FIPS PUB 186-4, "Digital Signature Standard (DSS)," July 2013.	Acceptable
Elliptic Curve Digital Signature Algorithm (ECDSA) or Edwards-curve Digital Signature Algorithm (EdDSA): len(n) ≥ 224 NIST FIPS PUB 186-4, "Digital Signature Standard (DSS)," July 2013.	Acceptable

4.2.3 Message Authentication

Message Authentication Code (MAC) algorithms are used to provide security services for data authentication and ***integrity***. They are used to establish the origin of information in a two-way exchange and confirms that information was not changed after it was transmitted. MAC algorithms must adhere to the specifications in Table 4-3.

Table 4-3. Approval Status of Algorithms for MAC Generation and Verification	
Algorithm Reference	**Use**
Keyed-Hash Message Authentication Code (HMAC): Key Lengths ≥ 112 bits NIST FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code (HMAC)," July 2008. NIST SP 800-107 Revision 1, "Recommendation for Applications Using Approved Hash Algorithms," August 2012.	Acceptable
Cipher-based Message Authentication Code (CMAC): AES NIST SP 800-38B, "Recommendation for Block ***Cipher*** Modes of Operation: The CMAC Mode for Authentication," October 2016.	Acceptable
Galois Message Authentication Code (GMAC): AES NIST SP 800-38D, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," November 2007.	Acceptable
KECCAK Message Authentication Code (KMAC): Key Lengths ≥ 112 bits NIST SP 800-185, "SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash," December 2016.	Acceptable

4.2.4 Secure Hashing

A secure ***hash algorithm*** can be used to support implementation of keyed-hash message authentication, digital signature algorithms, key derivation functions and random number generators. Cryptographic modules that use a secure hash algorithm shall adhere to the specification in Table 4-4.

Table 4-4. Approval Status of Hash Functions	
Algorithm Reference	**Use**
Secure Hash Algorithm (SHA)-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256) NIST FIPS PUB 180-4, "Secure Hash Standard (SHS)," August 2015.	Acceptable
SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512) NIST FIPS PUB 202, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," August 2015.	Acceptable

4.3 Cryptographic Key Security

Documents describing all implementation aspects of cryptographic key generation and management by the security service shall be kept confidential and are considered a "security record" for the purposes of Ohio Revised Code 149.433. These documents contain information directly used for protecting or maintaining the security of public office against attack, interference or sabotage and must be adequately protected using strong cryptographic methods.

4.4 Exceptions to the Standard

There are no exceptions to this State of Ohio IT standard.

5.0 References

5.1 Ohio Administrative Policy IT-01, "Authority of the State Chief Information Officer to Establish Ohio IT Policy," defines the authority of the state CIO to establish State of Ohio IT standards as they relate to the acquisition and use of information technology by state agencies, including, but not limited to, hardware, software, technology services and security.

5.2 Ohio Revised Code Section 149.433 exempts security and infrastructure records from public record requests.

5.3 Rule 123:3-1-01 of the Ohio Administrative Code, establishes the minimum requirements for creating, maintaining and using electronic signatures and records; the type, manner and format of electronic signatures; and security processes and procedures.

5.4 NIST Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules, Annex A, Approved Security Functions for FIPS PUB 140-2," includes a list of approved security functions for encryption (symmetric key), digital signatures, message authentication, hashing and random number generators.

5.5 NIST FIPS Publication 140-3, "Security Requirements for Cryptographic Modules," modernizes the previous standard (FIPS Pub 140-2) and essentially makes the U.S. standard a "pointer," indicating that the international standard, ISO 19790:2012, "Information technology — Security techniques — Security requirements for cryptographic modules," indicating that manufacturers should now use the international standard, which NIST helped to develop.

5.6 NIST FIPS PUB 180-4, "Secure Hash Standard (SHS)," specifies secure hash algorithms.

5.7 NIST FIPS PUB 186-4, "Digital Signature Standard (DSS)," specifies algorithms for applications requiring a digital signature, rather than a written signature.

5.8 NIST FIPS Publication 197, "Advanced Encryption Standard (AES)," specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.

5.9 NIST FIPS Publication 202, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," specifies the Secure Hash Algorithm-3 (SHA-3) family of functions on binary data.

5.10 NIST FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code (HMAC)," describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions.

5.11 NIST SP 800-38B, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," specifies a message authentication code (MAC) algorithm based on a symmetric key block cipher.

5.12 NIST SP 800-38D, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," is the fourth part in a series of recommendations regarding modes of operation of symmetric key block ciphers.

5.13 NIST SP 800-107 Revision 1, "Recommendation for Applications Using Approved Hash Algorithms," provides security guidelines for achieving the required or desired ***security strengths*** when using cryptographic applications that employ the approved hash functions specified in FIPS 180-4.

5.14 NIST SP 800-185, "SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash," specifies four types of SHA-3-derived functions: cSHAKE, KMAC, TupleHash, and ParallelHash, each defined for a 128- and 256-bit security strength.

6.0 Definitions

Asymmetric Key Cipher	A cryptographic algorithm that uses two encryption keys: the private key, which is never shared and is used when the data is encrypted, and the public key, which is shared and used when the data is decrypted. One drawback with asymmetric key ciphers is that they can be more computationally intense than comparably secure symmetric ciphers. Therefore, requiring more resources to achieve the same security.
Cipher	A cryptographic algorithm used to encrypt or decrypt data.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [1]

[1] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April 2013 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

Cryptographic Algorithm	A computational procedure that takes variable inputs, including a cryptographic key, and produces an output intended to implement a security function. There are three classes of cryptographic algorithms: hash functions, symmetric key ciphers and asymmetric key ciphers. These are defined by the number of cryptographic keys used with the algorithm (0, 1, or 2, respectively).
Cryptographic Module	A combination of hardware, software and firmware that implements a security service using one or more cryptographic algorithms.
Cryptographic Module Validation Program (CMVP)	Cryptographic Module Validation Program (CMVP) was established by NIST and the Communications Security Establishment (CSE) of Canada in July 1995. All cryptographic module testing under CMVP is handled by accredited third-party testing laboratories.
Cryptographically Strong	Describes a quality attribute of a security function that means, in comparison to other methods, the function has greater resistance against attack. Security functions approved in this standard are deemed cryptographically strong, in particular against attacks of brute force key search that intend to access the sensitive data protected by the specified algorithms.
Hash Algorithm	A function that maps a bit string of arbitrary length into a fixed length bit string. Secure hash functions are resistant to computational attacks that attempt to determine any input that maps to any pre-specified output.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.[2]
Message Authentication Code	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data.
National Institute of Standards and Technology (NIST)	National Institute of Standards and Technology (NIST) is a federal agency within the U.S. Department of Commerce

[2] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April 2013 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

	that establishes technology, measurement and national standards for information security as well as other areas.
Personally Identifiable Information (PII)	"Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes: • a name, identifying number, symbol, or other identifier assigned to a person, • any information that describes anything about a person, • any information that indicates actions done by or to a person, • any information that indicates that a person possesses certain personal characteristics.[3]
Security Service	A cryptography mechanism used to provide ***confidentiality***, data integrity, authentication, authorization or non-repudiation of information. A security service is often used to protect cryptographic keying material.
Security Strength	A "number" associated with the amount of work that is required to "break" a cryptographic algorithm or systems. In this standard, security strength is specified in "bits" such as the following: 128-bits or 160-bits.
Sensitive Data	Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of ***personally identifiable information*** that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, Criminal

[3] Based on Ohio Revised Code Section 1347.01 (E).

Justice Information under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy, and the Social Security Administration Limited Access Death Master File. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

Symmetric Key Cipher — A cryptographic algorithm that uses a single key to encrypt data. In practice, the two parties that encrypt and decrypt data must agree on the encryption key in advance. Symmetric key ciphers can be significantly faster than asymmetric key ciphers, but the necessity of exchanging keys increases their vulnerability.

7.0 Related Resources

Document Name
NIST Cryptographic Standards and Guidelines https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
NIST Cryptographic Module Validation Program (CMVP) Program https://csrc.nist.gov/projects/cryptographic-module-validation-program
NIST Special Publication 800-57, "Recommendation for Key Management – Part 1: General" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
NIST Special Publication 800-131A Revision 2, "Transitioning the Use of Cryptographic Algorithms and Key Lengths" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
NIST Special Publication 800-175A, "Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf
NIST Special Publication 800-175B Revision 1, "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf

8.0 Implementation

The requirements outlined in this standard shall be implemented within six months of the effective date of version 2.0 of the standard, 03/12/2021.

9.0 Revision History

This standard shall be reviewed no less than annually and updated as needed.

Date	Description of Change
07/25/2007	Version 1.0, Original Standard
03/12/2021	Revised to reflect advancements in encryption and cryptography standards. The template, branding, terminology and references were updated to align with current practices and publications.
10/13/2021	Conducted routine maintenance review of citations and references.
10/13/2022	Scheduled Standard Review

10.0 Inquiries

For information regarding this state IT standard, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor
Columbus, Ohio 43215

Telephone: 1.614.644.9391
Email: state.isp@das.ohio.gov
Web: infosec.ohio.gov

State of Ohio IT Standards can be found online at:
https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards

11.0 Attachments

None.