NEW YORK STATE | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S14-007
IT Standard: **Encryption**	**Updated:** 03/05/2025
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

Encryption is a cryptographic operation that is used to enhance security and protect the State's electronic information and data (collectively, "data") by transforming readable information ("plaintext") into unintelligible information ("ciphertext"). Encryption is an effective tool in mitigating the threat of unauthorized access to data.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], issued January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

3.0 Scope

This standard applies to all "State Entities" (SE), defined as "State Government" in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different standard, it must include the requirements set forth in this one. Where a conflict exists between this standard and an SE's standard, the more restrictive standard will take precedence.

4.0 Information Statement

SEs are responsible for the safekeeping of their data, one way to do this is through the use of encryption. The primary benefit of encryption is to ensure confidentiality, which is one of the three core concepts of information security. Employing robust encryption also helps to maintain data integrity, ensure data privacy requirements, and is often required to meet statutory and regulatory requirements.

The data that is to be encrypted is based on its information classification, risk assessment results, and use case of the data. An example use case is data used to authenticate the identity of an individual or process (e.g., PIN, password, passphrase). This data must be encrypted when stored, transported, or transmitted due to its sensitive nature. Another example use case is the encryption deployed when accessing an online bank account. Without proper encryption, the data sent back and forth could be easily obtained and used for unauthorized purposes.

Encryption products for confidentiality of data at rest and data in transit must incorporate Federal Information Processing Standard (FIPS) approved algorithms for data encryption. Approved encryption algorithms are contained in Appendix A. Use of outdated, cryptographically broken, proprietary encryption algorithms/hashing functions is prohibited.

Hashing algorithms transform a digital message into a short representation for use in digital signatures and other applications to validate the integrity of the message. They can also be used for multiple purposes including but not limited to, digital signatures, message authentication codes, key derivation functions, and pseudo random functions.

While hash functions may provide a certain amount of security strength, they do not meet all security requirements that keyed-hash functions provide.

For more information, refer to National Institute of Standards and Technology (NIST) Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms, and Appendix A. Where there is conflict between NIST 800-107 and Appendix A, the stronger function must be used.

Encryption products must be validated by the NIST Cryptographic Module Validation Program (CMVP) and operated in FIPS mode. The CMVP validates cryptographic modules to FIPS cryptography-based standards. Refer to Appendix B - Guidance in Selecting FIPS 140 Validated Products for information.

The current requirement is to use the FIPS 140-2 standard or better. FIPS 140-2 is valid until September 21, 2026; however, FIPS 140-3 validated products are already available and are strongly preferred over FIPS 140-2, where technically feasible.

Attention must be given to the regulations and national restrictions (e.g., export controls) that may apply to the use of cryptographic techniques in different parts of the world. The US Government restricts the export, disclosure, or release of encryption technologies to foreign countries or foreign nationals, including "deemed exports" to foreign nationals within the United States (excluding those foreign nationals with permanent resident visas (e.g., Green Cards), US citizenship, or 'protected person' status). SEs should consult with the counsel's office on these regulations and restrictions.

Per NYS-S13-001 - Secure System Development Life Cycle, a system's security plan must include documentation to show appropriate review of encryption methodologies and products. This will demonstrate due diligence in choosing a method or product that has received substantial positive review by reputable third-party analysts.

4.1 Data in Transit

Encryption is required for data in transit in the following situations:

1. When electronic Personal, Private or Sensitive Information (PPSI) is transmitted (including, but not limited to, e-mail, File Transfer Protocol (FTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).
2. When encryption of data in transit is prescribed by law or regulation.
3. When connecting to the State internal network(s) over a wireless network.
4. When remotely accessing the State internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network.
5. When data is being transmitted with an SE public facing website and/or web service, it is required to utilize Hypertext Transfer Protocol Secure (HTTPS) or Secure File Transfer Protocol (SFTP) in lieu of Hypertext Transfer Protocol (HTTP) or File Transfer Protocol (FTP) where technically feasible. SE public facing websites must utilize HTTP Strict Transport Security (HSTS), automatically redirecting HTTP requests to HTTPS websites where technically feasible.

Appropriate encryption methods for data in transit include, but are not limited to, Transport Layer Security (TLS) 1.2 using only currently valid and non-deprecated suites, Secure

Shell (SSH) 2.0 or later, Wi-Fi Protected Access(WPA) version 2 or later (with WiFi Protected Setup disabled) and encrypted Virtual Private Networks (VPNs). Components should be configured to support a FIPS-validated cipher suite. Ciphers and protocols that are deprecated or not compliant with this standard must not be used and must be disabled. If equivalent options exist for encryption in-transit, then to promote interoperability with other network and security devices industry standard protocols such as TLS should be selected over proprietary protocols.

Encryption for data in transit must be performed at the application level, or as close to the application level as possible. Network level encryption must not be used as a replacement for application-level encryption, except when used as a compensating control due to the use of insecure or legacy protocols that do not natively support encryption. Note that this does not preclude the use of encrypted VPNs when required for other purposes.

To ensure data protection, SEs shall support TLS 1.3 for both government-only and citizen or business-facing applications. In general, servers that support TLS 1.3 should be configured to use TLS 1.2 as well. However, TLS 1.2 may be disabled on servers that support TLS 1.3 if it has been determined that TLS 1.2 is not needed for interoperability. Please see NIST 800-52 Rev 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, or its successor.

4.2 Data at Rest

Data at rest refers to data that has been stored on a given device. Regardless of infrastructure, location, or device ownership, encryption is required for data at rest, as follows:

- Desktops, laptops, and any other devices that contain SE PPSI;
- Data stores (including, but not limited to, databases, cloud, and file shares) that contain SE PPSI;
- All mobile devices, whether State issued or third-party, that contain any SE data;
- All portable storage devices containing any SE data; and
- When electronic PPSI is transported or stored outside of a State facility.

Full Disk encryption is required for all State devices that access or contain SE data.

All encryption products deployed on laptops and other portable devices, must use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot. Devices that do not have TPM, must use some other form of pre-boot authentication such as the Apple T2 chip or FileVault.

To mitigate attacks against encryption keys, when outside of State facilities, SE laptops and third-party laptops that access or contain SE PPSI must be powered down (i.e., shut down or hibernated) when unattended.

SEs must have a process or procedure in place for confirming devices and media have been successfully encrypted using at least one of the following, listed in preferred order:

1. automated policy enforcement;
2. automated inventory system; or
3. manual record keeping.

4.3 Key Management

The SE must ensure that a secure environment is established to protect the cryptographic keys used to encrypt and decrypt information. Keys must be securely distributed and stored.

Access to keys must be restricted to only individuals who have a business need to access the keys.

Unencrypted keys must not be stored with the data that they encrypt.

Keys will be protected with an authentication token that conforms to the identified assurance level as per NYS-P20-001 - Digital Identity Policy.

Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted. If a compromise has been discovered, a new key must begenerated and used to continue protection of the encrypted information. Specific circumstances should be evaluated to determine if a breach notification is required.

Encryption keys and their associated hardware and software products must be maintained for the life of the archived data that was encrypted with that product.

4.4 Cryptographic Asset Inventory

The SE must develop an inventory of all cryptographic systems currently deployed by the SE or on the SE's behalf, including where and for what purpose the cryptographic systems are used, and the use characteristics. The inventory must encompass all the following algorithms. See the table below:

Algorithm	Function	Specification
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A/B/C
Menezes-Qu-Vanstone (MQV) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A/B/C
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithms used for digital signatures	FIPS PUB 186-4

Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526
RSA Signature Algorithm	Asymmetric algorithm used for key establishment	FIPS SP 800-56B Rev. 1
Digital Signature Algorithm	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4
Advanced Encryption Standard (AES)	Symmetric algorithm used for data encryption	FIPS 197
Triple Data Encryption Standard (3DES)	Symmetric algorithm used for data encryption	NIST SP 800-67 Rev. 2
Secure Hash Algorithm (SHA)	Hash algorithm used for one-way hashing of data	FIPS 180-4 and FIPS 202
Other Asymmetric Algorithms, Symmetric Algorithms, Hash Algorithms, and other cryptographic systems	Remaining algorithms not enumerated in the list above	Not applicable

For each information system or asset, the Cryptographic Asset Inventory must include at least the following information:

1. Each cryptographic system actively used by the information system or asset, including the:
    a. Cryptographic algorithm used
    b. Service provided by the cryptographic system; and
    c. Length of associated cryptographic keys or modules
2. If the cryptographic system(s) is/are part of a software package, indicate whether the software package is
    a. Commercial-Off-the-Shelf (COTS) and name of the vendor;
    b. Government-Off-the-Shelf (GOTS) and name of the vendor; or
    c. Other (e.g., custom software) and name of the vendor/developer
3. Operating system(s), including major and minor version information, if applicable.
4. Whether the information system or hosting information system(s) is/are hosted by:
    a. The SE (on premise);
    b. A commercially operated cloud service provider, in which case the name of the commercial provider must be supplied;
    c. A Government-operated cloud service provider, in which case the name of the agency provider must be supplied; or
    d. A hybrid environment, in which case the name of the cloud service provider(s) must be supplied.

5. This inventory must be maintained, but may be part of other inventories or system documentation maintained by the SE. The minimum requirements outlined in this standard must be met and the protections afforded must be appropriate.
6. The Cryptographic Asset Inventory must be kept updated and accurate due to system upgrades, changes, or other modifications that affect the contents of the inventory.

SEs may withhold certain information of the inventory from public disclosure pursuant to Article 6 or 6-A of the Public Officers law, including but not limited to, if it is deemed that disclosure of the information would jeopardize the capacity to guarantee the security of information technology assets, would interfere with a law enforcement investigation or reveal criminal investigative techniques or procedures, or would endanger the life or safety of a person.

When enumerating cryptographic systems, SEs should keep in mind that an information system or asset often contains multiple cryptographic systems. They should also note that unused or inactive cryptographic systems should not be included in this inventory. An unused or inactive cryptographic implementation is one that is not, at the time of the agency inventory, actively used for creation and exchange of encryption keys, encrypted connections, or creation and validation of digital signatures.

Cryptographic Asset Inventories should be completed no later than 1 year from the publication date of this standard and updated at least annually thereafter. Inventories should be stored with security protections and controls appropriate to the sensitivity of their contents.

The Cryptographic Asset Inventory should be used in conjunction with other sources of information to assist the SE in transitioning from cryptographic algorithms vulnerable to a Cryptically Relevant Quantum Computer (CRQC), for post-quantum digital signature algorithms and key-establishment schemes.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required. If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Chief Information Security Office exception process.

The Cryptographic Asset Inventory specified in Section 4.4 of this standard shall be effective one (1) year after the latest publication date of this standard.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in the ITS Glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S14-007
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/policies

8.0 Revision History

This policy document should be reviewed consistent with the requirements set forth in ITS-P24-003 Process for Establishing Information Technology Polices, Standards and Guidelines.

Date	Description of Change	Reviewer
03/21/2014	Original Standard Release; *replaces CSCIC/OCS Cryptographic Controls (S10-006) and Key Management Standards (S10-007) and ITS Encryption Standard (ITS-S07-001)*	Thomas Smith, Chief Information Security Officer
03/20/2015	Allow for UEFI Secure Boot in place of pre- boot authentication. Require TPM for pre-boot authentication. Minor wording clarifications. Updated key length for ECDSA and SHA from 224 to 256 in Appendix A.	Deborah A. Snyder, Deputy Chief Information Security Officer
03/15/2016	Require all websites and web services within scope to be accessible through a secure connection (HTTPS). Revised TLS 1.1 to 1.2	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer

06/26/2017	Add Appendix C - Minimum Browser Support	Deborah A. Snyder, Acting Chief Information Security Officer
07/16/2020	Update revised Scope and Authority and update links from Identity Assurance to Digital Identity	Karen Sorady, Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer
03/05/2025	Scheduled review and updates, Removal of Appendix C – Minimum Browser Requirements, Added TLS 1.3 regulations along with implementations dates, Clarified statements around full disk encryption methodologies.	Chris DeSain, Chief Information Security Officer

9.0 Related Documents

NIST Special Publication 800-52, Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

NIST Special Publication 800-57, Part 1, Recommendation for Key Management – Part 1: General

NIST Federal Information Processing Standard (FIPS) Publication 140-3

NIST Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms

NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

APPENDIX A - Approved Algorithms

Algorithm	Minimum Key Length	Use Case
AES	128	Data Encryption
RSA	2048	Digital Signatures Public Key Encryption
ECDSA	256	Digital Signature Public Key Encryption
SHA	256	Hashing
HMAC SHA1	112	Keyed-Hash Message Authentication Code

APPENDIX B – Guidance for Selecting FIPS 140 Validated Products

All government agencies that use cryptographic-based systems to protect Personal, Private or Sensitive Information (PPSI), need to have a minimum level of assurance that the product's stated security claim is valid.

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) cryptography-based standards.

The list of FIPS validated cryptographic modules can be found on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/validation.html. The list can be searched by vendor or by year of validation.

It is important to note that the items on this list are cryptographic modules which may either be an embedded component of a product or application, or a complete product in and of itself. In addition, it is possible that vendors who are not found on this list might incorporate a validated cryptographic module from this list into their own products and components.

When selecting a product from a vendor, verify that the application or product that is being offered is either a validated cryptographic module itself (e.g., full disk encryption solution, SmartCard) or the application or product uses an embedded validated cryptographic module (toolkit, etc.) by confirming the module's validation certificate number. Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module which provides all the cryptographic services in the solution and references the module's validation certificate number. This number can be checked against the CMVP validation list. If the number does not match, the vendor is not offering a validated solution. Be aware that vendors may sometimes make invalid conformance claims such as:

- The module has been designed for compliance to FIPS 140-3.
- The module has been pre-validated and is on the CMVP pre-validation list.
- The module will be submitted for testing.
- The module has been independently reviewed and tested to comply with FIPS 140-3.
- The module meets all the requirements of FIPS 140-3.
- The module implements FIPS Approved algorithms; including having algorithm certificates.
- The module follows the guidelines detailed in FIPS 140-3.

A cryptographic module does not meet the requirements or conform to the FIPS standard unless a reference can be made to the validation certificate number.

Users must also be cognizant of the version number of the validated cryptographic module and, for software products, the operating systems that it has been tested on. Only the version numbers listed in the Cryptographic Module column of the CMVP list are FIPS validated and only when run on the operating systems listed in the

Level/Description column.

FIPS Mode

Many validated products have the capability to operate in FIPS mode, as well as non-FIPSmode. Operating in FIPS mode will ensure that the module uses only FIPS approved encryption algorithms.

Vendors provide a "Security Policy" as part of their module/product validation. This "Security Policy" can be found under the Cryptographic Module column on the CMVP list. The "Security Policy" will provide information on how to configure the module in a FIPS mode ofoperation and how the module functions to meet the FIPS requirements.

Modules in Process

NIST maintains a Modules in Process list. Inclusion on the list is at the option of the vendor. Posting on this list does not imply a guarantee of final FIPS validation. Therefore, SEs that deploy a module before it is validated incur a level of risk in that the module may never be validated, or the version submitted for testing is not the version that is validated.