cisecurity **Information Technology Standard**	**No:**
IT Standard: **Encryption**	**Updated:**
	Issued By: **Owner:**

1.0 Purpose and Benefits

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

3.0 Scope

This standard applies to all systems, which includes websites and web services, for which the entity has administrative responsibility, including those managed and hosted by third-parties on behalf of the entity.

4.0 Information Statement

The need for encryption of information is based on its classification, risk assessment results, and use case.

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 U.S. 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 (i.e., Green Cards), U.S. citizenship, or 'protected person' status). If you have any questions, please contact Counsel and Legal Services.

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.

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

Although hash functions such as SHA 1, provide a certain amount of security strength, it does not meet all security requirements for keyed-hash functions such as HMAC SHA 1. Refer to FIPS 180-4 for more information on different types of application hashing algorithms as well as Appendix A.

Hashing algorithms can be used for multiple purposes including but not limited to, digital signatures, message authentication codes, key derivation functions, pseudo random functions.

Approved hashing functions are contained in Appendix A.

Use of outdated, cryptographically broken, proprietary encryption algorithms/hashing functions is prohibited.

Due to the prevalence of incorrectly implemented cryptography, encryption products must have FIPS 140 (Security Requirements for Cryptographic Modules) validation and be operated in FIPS mode. Refer to Appendix B - Guidance in Selecting FIPS 140 Validated Products for further information.

Electronic information used to authenticate the identity of an individual or process (i.e., PIN, password, passphrase) must be encrypted when stored, transported or transmitted. This does not include the distribution of a one-time use PIN, password, passphrase, token code, etc., provided it is not distributed along with any other authentication information (e.g., user-ID).

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 personally identifying information (PII) 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 internal network(s) over a wireless network.

4. When remotely accessing an entity's internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network. This does not apply to remote access over an entity's managed point to point dedicated connection.

5. When data is being transmitted with an entity's public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP) where technically

feasible. Public facing websites must utilize HTTP Strict Transport Security (HSTS), automatically redirecting HTTP requests to HTTPS websites where technically feasible. Minimum browser support is listed in Appendix C.

Appropriate encryption methods for data in transit include, but are not limited to, Transport Layer Security (TLS) 1.2 or later, 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 the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.

4.2 Data at Rest

Encryption is required for data at rest, as follows:

1. For the systems listed below:
   a. desktops that access or contain personally identifying information (PII);
   b. data stores (including, but not limited to, databases, file shares) that contain PII;
   c. all mobile devices, whether entity issued or third-party, that access or contain any entity information; and
   d. all portable storage devices containing any entity information.
2. When electronic PII is transported or stored outside of the entity facility.

Full disk encryption is required for all issued laptops that access or contain entity information. Full disk encryption products must use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.

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

The entity 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 entity 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.

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 be generated 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 software products must be maintained for the life of the archived data that was encrypted with that product.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer’s exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

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

cisecurity@cisecurity.com

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	**Description of Change**	**Reviewer**

9.0 Related Documents

NIST Federal Information Processing Standard (FIPS) Publication 140-2

NIST Federal Information Processing Standard (FIPS) Publication 198-1

NIST Federal Information Processing Standard (FIPS) Publication 180-4

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

APPENDIX C – Minimum Browser Support

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 SHA 1	112	Keyed-Hash Message Authentication Code