

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

29.01.03.Z1.07 Encryption

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

The purpose of this policy is to provide Texas A&M University System Health Science Center (HSC) guidance on the use of encryption to protect HSC information resources that contain, process, or transmit confidential information. Additionally, this policy provides direction to ensure that State and Federal regulations are followed.

1.2 Audience

This policy applies to all HSC employees and affiliates, including contractors. It addresses encryption policy and controls for confidential data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management. This policy is compatible with, but does not supersede or guarantee compliance with all State and federal encryption standards.

HSC will identify the owners and locations of confidential data through its annual data protection risk assessment process. HSC can use this risk assessment to determine the proper encryption implementation(s) to achieve the desired level of protection.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic

file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code (TAC) 202, Information Security Standards.

1.5 Definitions

- **Advanced Encryption Security (AES):** A FIPS approved, block cipher (See: **Rijndael**), symmetric key adopted as an encryption standard by the U.S. government. AES has 128, 196, and 256 key lengths, making it very secure. Data stored with AES cannot be decrypted without the key. [NIST FIPS 197, Advanced Encryption Standard (AES), November 2001].
- **ARCFOUR (ARC4):** See **RC4 Encryption**.
- **Asymmetric Encryption (or Public Key Cryptography (PKC) or Public Key Encryption):** A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (a public and a private key). Only one key (the private key) must be kept secret. The key that is exchanged (the public key) poses no risk if it becomes known.
- **Authentication, Authorization, and Accounting (AAA) Key (AAAK), or Master Session Key, (MSK):** Keying material that is derived between the Extensible Authentication Protocol (EAP) peer and the server and exported by the EAP method. The key is at least 64 octets in length. In existing implementations, an AAA server acting as an EAP server transports the key to the authenticator
- **Binding:** The process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.
- **Block Cipher:** A methodology that encrypts one block of data at a time.
- **Blowfish:** A freeware, symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It has a 64-bit block size and a variable key length from 32 to 448 bits.
- **Bulk Encryption:** Simultaneous encryption of all channels of a multichannel (multiplexed) telecommunications link.
- **CAST-128 (or CAST5):** A block cipher created by Carlisle Adams and Stafford Tavares. Some encryption products use CAST-128 as the default cipher. CAST-256 was an AES candidate.
- **Certificate:** See **Digital Certificate**.

- **Certification Authority (CA):** A trusted entity authorized to create, sign, and issue (Certification Authority) public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate (e.g., control of the registration process, the identification and authentication process, the certificate manufacturing process, and publication, revocation, renewal and archival of certificates.) The CA certifies the user's identity and association with private and public keys.
- **Certificate-Based Authentication:** The use of SSL and certificates to authenticate and encrypt HTTP traffic.
- **Certificate Management:** Process whereby certificates are generated stored, protected, transferred, loaded, used, and destroyed.
- **Certificate Revocation List (CRL):** List of invalid certificates that have been revoked by the issuer.
- **Cipher:** Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.
- **Cipher Block Chaining (CBC):** A mode of operation for a block cipher using an initialization vector (IV) of a certain length and a chaining mechanism that causes the decryption of a block of ciphertext to depend on all the preceding ciphertext blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous ciphertext block. A single bit error in a ciphertext block affects the decryption of all subsequent blocks. Rearrangement of the order of the ciphertext blocks causes decryption to become corrupted.
- **Cipher Block Chaining Message Authentication Code (CBC-MAC):** A technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the block before it. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.
- **Cipherlock:** A Mechanical lock that accepts a specific key sequence to grant access.
- **Ciphertext:** The encrypted form of the message being sent.
- **Cipher Text Auto-Key (CTAK):** Cryptographic logic that uses previous ciphertext to generate a key stream.

- **CipherText Stealing (CTS):** A general method of using a block cipher mode of operation that processes messages that are not evenly divisible into blocks without resulting in any expansion of the ciphertext, at the cost of slightly increased complexity.
- **Ciphony:** Process of enciphering audio information, resulting in encrypted speech.
- **Common Criteria (CC):** An international information technology security evaluation (ISO/IEC 15408) for computer security. It is often associated with an Evaluation Assurance Level (EAL).
- **Communications Security (COMSEC):** Measures and controls taken to deny unauthorized access to information derived from telecommunications and to ensure the authenticity of such telecommunications, including crypto-security, transmission, emission, and physical security of COMSEC material.
- **Confidential Information:** Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act) and other constitutional, statutory, judicial and legal agreements.
- **Counter Mode with Cipher Block Chaining MAC Protocol (CCMP):** A data confidentiality and integrity protocol that may be negotiated as a cipher suite for the protection of user traffic in a Robust Security Network (RSN) environment. Like TKIP, CCMP was developed to address all known inadequacies of WEP without the constraint of requiring the use of existing hardware. CCMP is mandatory for RSN WLAN compliance.
- **Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode:** An “authenticate-and-encrypt” block cipher mode of AES. It is an authenticated encryption algorithm that combines the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) algorithm to provide both authentication and integrity protection (privacy). CCM mode is only defined for 128-bit block ciphers, e.g., 128-bit AES.
- **Cryptography:** The art and science of keeping information secure. It deals with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages including: Asymmetric (or public-key) encryption; Symmetric (or private key) encryption; and Elliptic curve cryptography:
- **Cryptographic Algorithm:** A Well defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic

processes such as encryption/decryption, key generation, authentication, and signatures.

- **Crypto Ignition Key (CIK):** A device or electronic key used to unlock the secure mode of crypto-equipment.
- **Cryptonet:** A network of stations holding a common key.
- **Cryptoperiod** (key lifetime or validity period): A specific time span during which a cryptographic key setting remains in effect. When the cryptoperiod ends, the key is no longer available for either encryption or decryption. A cryptoperiod may include the span of time (decades) that keys are needed for archived data. The cryptoperiod also may represent a maximum volume of data.
- **Crypto-virus:** A virus or worm that encrypts the victim's data with a strong algorithm (e.g., RSA 1,024-bit encryption) so the victim can't unscramble it without paying a ransom for a "decryptor."
- **Data Encryption Standard (DES):** The former U.S. Government standard using a private, symmetric-key cryptographic algorithm. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. In 2005, the Secretary of Commerce withdrew federal approval for DES because it “no longer provides the security that is needed to protect Federal government information” (withdrew: FIPS 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation).
- **Data Owner:** The designated manager within HSC who is responsible for the business function that is supported by the information resource. This responsibility may be assigned to the person who is responsible for the business results of that system or the business use of the information. The data owner is responsible for establishing controls that address the risks to the security (confidentiality, integrity, availability) of assigned information resources. While the Office of Information Technology (OIT) Director or IRM may be responsible for maintaining the physical inventory of OIT assets, the IRM is not typically the owner or user of the information that resides within those assets.
- **Decapsulation:** The process to strip off one IP stack layer's headers and pass the rest of the packet up to the next higher layer on the protocol stack, while recovering the content of protected frames—that is, to decrypt a received ciphertext packet. During decapsulation, various validation checks are performed on the frames which could result in discarding inappropriate frames.

- **Decipher (or Decrypt):** Convert enciphered text or data to a readable form or plain text by means of a cryptographic system.
- **Diceware:** A method for creating passphrases, passwords, and other cryptographic variables using ordinary dice as a hardware random number generator. For each word in the passphrase, five dice rolls are required. The numbers that come up in the rolls are assembled as a five digit number. That number is then used to look up a word in a word list.
- **Diffie-Hellman Key:** A technique of changing encryption techniques on the fly by exchanging private keys using a public key management methodology.
- **Digital Certificate:** A digital representation of information that establishes credentials for conducting transactions on the Web by binding the user's identification with the user's public key in a trusted manner. At minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
- **Digital Signature:** Cryptographic process (hash) used to uniquely identify the sender of the message and prove the message or the signer of a document, has not changed since transmission by assuring message originator authenticity, integrity, and non-repudiation. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.
- **Digital Signature Algorithm (DSA):** An asymmetric cryptosystem that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.
- **Digital Signature Standard (DSS):** The US Government standard that specifies the DSA asymmetric cryptographic system.
- **Electronically Generated Key:** A key generated in a COMSEC device by introducing a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key.
- **Electronic Key Management System (EKMS):** Interoperable collection of systems to automate the planning, ordering, generating, distributing, storing, filing, using, and destroying of electronic key and management of other types of COMSEC material.

- **Elliptic Curve Cryptography:** A newer public-key cryptosystem that potentially can provide comparable levels of security but with faster calculations using smaller key sizes than the older methods. It provides effective security of roughly half its respective key length.
- **Encapsulation:** The inclusion of data structure from an upper layer protocol in a lower layer protocol so that the first data structure is hidden for the time being.
- **Encryption (encrypt, encipher, or encode):** The conversion of plaintext information into a code or ciphertext using a variable, called a “key” and processing those items through a fixed algorithm to create the encrypted text that conceals the data’s original meaning.
- **Encryption Algorithm:** A formula used to convert information into an unreadable format. The strength of an algorithm is related to its ability to maximize entropy instead of its secrecy. These algorithms are generally made public and subject to peer review. Examples of public algorithms are AES, DES and Triple DES, and RSA.
- **Extensible Authentication Protocol (EAP):** A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences. The EAP provides some common functions and a negotiation of the desired authentication mechanism that are called EAP methods. There are about 40 different methods including: EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS (Transport Layer Security), EAP-IKEv2, EAP-SIM, and EAP-AKA. Common wireless networks methods include: EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP and EAP-TTLS (Tunneled Transport Layer Security).
- **Extraction Resistance:** The capability of crypto-equipment or secure telecommunications equipment to resist efforts to extract the crypto key.
- **Encryption (or Key) Strength:** The strength of the encrypted text is determined by the entropy, or degree of uncertainty, in the key and the algorithm. Key length and key selection criteria are important determinants of entropy. Greater key lengths generally indicate more possible keys. More important than key length, however, is the key selection criteria. The full 128 bits of entropy will only be realized if the key is randomly selected across the entire 128-bit range. A key should be large enough that a brute force attack (possible against any encryption algorithm) is infeasible. Depending upon the algorithm (symmetric, asymmetric, elliptical curve), it is usual to have different key sizes for the same level of security, For example, the security available with a 1024-bit key using asymmetric RSA is approximately equal in security to an 80-bit key in a symmetric algorithm.

- **Evaluation Assurance Level (EAL):** A numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs) which covers the complete development of a product, with a given level of strictness. Common Criteria has seven EAL levels, with higher EALs indicating that the claimed security assurance has been more extensively validated, but not guaranteeing better security.
- **Fair Cryptosystem:** See **Key Escrow**.
- **Federal Information Processing Standards Publication (FIPS PUB 140), Security Requirements for Cryptographic Modules:** Federal standards for cryptographic algorithms (e.g., AES, 3DES (TDEA), Diffie-Hellman, RSA, RC5 and IDEA).
- **File Encryption Key (FEK):** A fast symmetric algorithm that encrypts file data. The FEK is a randomly generated key of a certain length required by the algorithm, or by law if the algorithm supports variable length keys.
- **Four-Way Handshake:** An authentication process that establishes a key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: Pairwise Master Key (PMK), Access Point (AP) nonce (ANonce), Station (STA) nonce (SNonce), AP MAC address and STA MAC address.. The product is then put through a cryptographic hash function. The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic.. The earlier EAP exchange has provided the shared secret key PMK. This key is designed to last the entire session and should be exposed as little as possible.
- **Full disk encryption (FDE) (or Whole Disk Encryption):** A kind of disk encryption software or hardware which encrypts every bit of data that goes on a disk or disk volume. The term "full disk encryption" is often used to signify that everything on a disk, including the programs that can encrypt bootable operating system partitions, but they must still leave the Master Boot Record (MBR), and thus part of the disk, unencrypted.
- **Full Volume Encryption (FVE):** A method for encrypting a single partition, either physical or virtual, on a hard drive. It is different than Full Disk Encryption since parts of the disk are left unencrypted
- **Hash or (Hash Function):** A cryptographic output that maps a variable-length data block or message into a fixed-length value called a message digest or hash code. Hashes are used to verify file and message integrity. A hash, by definition, is a one-way encryption. An attacker who obtains the password cannot run the hash through an algorithm to decrypt the password.

- **Hash Message Authentication Code (HMAC) or Keyed-HMAC (KMAC):** A type of message authentication code (MAC) that uses a cryptographic hash function in combination with a secret key. It can simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA-1. For example, MD5 and SHA-1 operate on 512-bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (128 or 160 bits in the case of MD5 or SHA-1, respectively), although it can be truncated if desired. Truncating the hash image reduces the security of the MAC. FIPS PUB 198 generalizes and standardizes the use of HMACs. HMAC-SHA-1 and HMAC-MD5 are used within the IPsec and TLS protocols.
- **Hybrid Encryption:** An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.
- **Information Resources Manager (IRM):** Responsible to the State of Texas for management of the institution's information resources. The designation of an institution information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state institution's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of the institution. If an institution does not designate an IRM, the title defaults to the institution's President, and the President is responsible for adhering to the duties and requirements of an IRM.
- **Information Security Officer (ISO):** Responsible to the executive management for administering the information security function within the institution. The ISO is the institution's internal and external point of contact for all information security matters.
- **Institute of Electrical and Electronics Engineers (IEEE) 802.11:** A set of standards for wireless LAN (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands. IEEE 802.11i standard supersedes WEP. The Wi-Fi Alliance implemented a WPA as a subset of 802.11i and refers to their approved, interoperable implementation of the full 802.11i as **WPA2**. IEEE 802.11i makes use of the AES block cipher, whereas WEP and WPA use the RC4 stream cipher.

- **Institution-Sensitive Data:** An optional, state entity defined category that also may be identified as: “Security-Sensitive,” “Privileged,” or “Protected.” This category of data may be subject to disclosure or release under the Public Information Act, but requires some level of protection. Note: Institution-sensitive data may include: operational information, personnel records, information security procedures, research, internal communications, contractual information, or other information that has constitutional, statutory, judicial, or legal agreement restrictions on access, disclosure, or release.
- **International Data Encryption Algorithm (IDEA):** A block cipher algorithm intended as a replacement for the Data Encryption Standard. IDEA is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES).
- **Internet Key Exchange (IKE):** The protocol used to set up a security association (SA) in the IPsec protocol suite. IKE uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.
- **Internet Protocol Security (IPsec):** A complex aggregation of protocols for security at the network or packet processing layer of network communication that provide authentication and confidentiality services to individual IP packets. It can be used to create a VPN over the Internet or other untrusted network, or between any two computers on a trusted network..
- **Kerberos:** A system developed at MIT that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.
- **Key:** A parameter that determines the functional output of a cryptographic algorithm. Without a key, the algorithm would have no result. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.
- **Key-Auto-Key (KAK):** Cryptographic logic using the previous key to produce the new key.
- **Keyed-HMAC (KMAC):** See **Hash Message Authentication Code (HMAC)**.
- **Key Encapsulation:** An encryption key recovery mechanism that encapsulates keys or key parts into key recovery block and is associated with ciphertext.

- **Key-Encryption-Key (KEK):** A cryptographic key that encrypts or decrypts another key for transmission or storage.
- **Key Escrow (Fair Cryptosystem):** An arrangement in which the keys needed to decrypt encrypted data are held in a key escrow database so that, under certain circumstances, an authorized third party may extract the key under two party control. The third party may include a trusted government entity that may need to access to employees' private communications, or be able to view the contents of encrypted communications. A key escrow system consists of the following components:
 - **Key Exchange:** The process by which the sender and the receiver exchange public keys and other information to encrypt or decrypt the messages they exchange with each other.
 - **Key Generation and Distribution:** The final step in authentication that permits secure data transfer through a 4-Way Handshake and a Group Handshake.
 - **Key Management:** The processes and procedures for providing the generation, distribution, tracking, control and destruction for all cryptographic key material, symmetric keys as well as public keys and their associated certificates.
 - **Key Management Infrastructure (KMI):** Framework and service that provide the generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic key material, including symmetric keys as well as public keys and public key certificates.
- **Key Pair:** Public key and its corresponding private key as used in public key cryptography.
- **Key Recovery:** A stage in the lifecycle of keying material that includes mechanisms and processes to allow authorized entities to retrieve keying material from key backup or archive.
- **Key Scope:** Data encrypted by a particular key, divided into equal-sized data units. The key scope is identified by three non-negative integers: tweak value corresponding to the first data unit, the data unit size, and the length of the data.
- **Key Strength:** See **Encryption Strength**.

- **Layer 2 Tunneling Protocol (L2TP):** An extension of the PPP protocol that allows the ISP to establish a VPN through Internet connections, as opposed to requiring direct access, e.g., via leased lines or direct dial-up connections.
- **Link Encryption:** A protocol that encrypts and decrypts all traffic at each end of a communications line (e.g. a teletype circuit).
- **Local Management Device/Key Processor (LMD/KP):** An EKMS platform providing automated management of COMSEC material and generating key for designated users.
- **Manual Remote Rekeying:** Procedure by which distant crypto-equipment is rekeyed eclectically, with specific actions required by the receiving terminal operator. Same as: cooperative remote rekeying.
- **Master Session Key (MSK):** See **Authentication, Authorization, and Accounting (AAA) Key (AAAK).**
- **Message Authentication Code (MAC):** A short piece of cryptographic information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*). The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content, and so should be called Message Authentication and Integrity Code: (MAIC).
- **Message-Digest algorithm 5 (MD5):** A widely used, but partially insecure cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.
- **Message Indicator:** Sequence of bits transmitted over a communications system for synchronizing crypto-equipment. Some off-line systems, such as the KL-51 and one-time pad systems, employ messages indicators to establish decryption starting points.
- **Message Integrity Code (MIC):** A short cryptographic checksum used to authenticate a message. It is also known as integrity check-values of modification detection code. MIC is different from MAC in that a secret key is not used in its operation. Although the terms are sometimes used interchangeably, a MIC should always be encrypted during transmission if it is to be used as a reliable gauge of message integrity. A MAC uses a secret key and does not necessarily need to be encrypted to provide the same level of assurance. A given message will always produce the same MIC assuming the same algorithm is used to generate both. Conversely, the same message can only generate matching MACs if the same secret key is used with the same

algorithms to generate both. Since MICs do not use secret keys, they are a less reliable gauge of message integrity. when not used with other authentication methods.

- **Message stream encryption (MSE)/Protocol encryption (PE), or Protocol header encrypt (PHE):** Related features of some peer-to-peer file-sharing clients, including BitTorrent clients. They attempt to make traffic harder to identify by third parties including ISPs. MSE/PE is implemented in Azureus, BitComet, BitTornado, KTorrent, Mainline, µTorrent, Transmission (v0.90) and rTorrent. PHE was implemented in old versions of BitComet. Similar protocol obfuscation is supported in up-to-date versions of some other (non-BitTorrent) systems.
- **Non-State Government Owned Computing Device:** Any device that is capable of receiving, transmitting, and/or storing electronic data and that is not owned or leased by or under the control of HSC.
- **On-line Cryptosystem:** A system that performs encryption and decryption in association with the transmitting and receiving functions.
- **One-Way Encryption:** Irreversible transformation of plaintext into cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.
- **Over-the-air Rekeying (OTAR):** Changing traffic encryption key or transmission security key in remote crypto-equipment by sending the new key directly to the remote crypto-equipment via the same communications path it secures.
- **Per-call Key:** Unique traffic encryption key generated automatically by certain secure telecommunication systems to secure single voice or data transmissions.
- **Point to Point Protocol (PPP):** A data link protocol commonly used to establish a direct connection between two nodes over serial cable, phone line, trunk line, cellular telephone, specialized radio links, or fiber optic links. Most Internet service providers use PPP for customers' dial-up access to the Internet. Two common encapsulated forms of PPP, Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA), are used in a similar role with Digital Subscriber Line (DSL) Internet service. PPP is commonly used to act as a data link layer protocol for connection over synchronous and asynchronous circuits,
- **Point to Point Tunneling Protocol (PPTP):** A network protocol that enables the secure transfer of data from a remote client to a private enterprise server

by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, VPN over public networks such as the Internet.

- **Portable Computing Device:** Any easily portable device that is capable of receiving, transmitting, and/or storing electronic data. This includes but is not limited to, notebook and tablet computers, handheld computers, personal digital assistants (PDAs), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, magnetic tapes, and similar removable media or storage devices.
- **Pre-Shared Key (PSK):** A static, symmetric key cryptographic algorithm such as a password which is entered to access a secure Wi-Fi system using WEP or WPA. Both the wireless access point (AP) and the client *share* the same key. In the Civil War, the Confederate Navy used a book cipher PSK. Each person had the same edition of a dictionary and replaced words in the plaintext of a message with the location of words from the book by page and line number.
- **Pretty Good Privacy (PGP):** A crypto-graphic privacy and authentication software that is used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications. It was originally created in 1991, PGP and other similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.
- **Private Key:** The part of a key pair that generates a digital signature and decrypts information, including key encryption keys during key exchange. It is computationally infeasible to determine a private key given the associated public key.
- **Proprietary Encryption:** An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
- **Protected Extensible Authentication Protocol (PEAP):** A method to securely transmit authentication information, including passwords, over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security and comes ready to run in Microsoft Service Packs (e.g., XP). PEAP is not an encryption protocol; it only authenticates a client into a network using server-side public key certificates to authenticate the server. It then creates an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information to authenticate the client is then encrypted and user credentials are safe from eavesdropping. PEAP can tunnel only EAP-type protocols such as EAP-TLS, EAP-MS-CHAPv2 and EAP-SIM.
- **Protocol encryption (PE):** See **Message stream encryption (MSE)**.

- **Protocol Header Encrypt (PHE):** See **Message stream encryption (MSE)**.
- **Public Information:** Information intended or required for public release as described in the Texas Public Information Act.
- **Public Key:** The Part of a key pair that is made public, usually by posting it to a directory. A public key can be either a signature or key exchange key. The signer's public signature key is used to verify a digital signature.
- **Public Key Certificate:** An electronic document that incorporates a digital signature and contains the identity of a user, the public key component of the user, and the name of the issuer who verifies that the public key belongs to the user. In a typical PKI scheme, the digital signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements").
- **Public Key Cryptography (PKC):** See **Asymmetric Cryptography**.
- **Public Key Encryption:** See **Asymmetric Cryptography**.
- **Public Key Forward Secrecy (PFS):** A property of asymmetric key agreement protocols that ensures that any session key that is derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.
- **Public Key Infrastructure (PKI):** A framework established to issue, maintain, and revoke public key certificates. PKI provides the capability to use unsecured public networks to securely and privately exchange data and money through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority. PKI uses a digital certificate that identifies an individual or organization and has directory services that can start and revoke the certificates.
- **Randomizer:** An analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for key generation or to provide a starting state for a key generator.
- **RC4 Encryption** (also known as **ARC4** or **ARCFOUR**): A widely-used software stream cipher that is used in protocols such as Secure Sockets Layer (SSL) to protect Internet traffic and WEP to secure wireless networks. It uses the 128-bit EAPOL-KEK derived from the PTK using the PRF. RC4 is vulnerable to attacks and is not FIPS-approved,
- **RC5 Encryption:** A block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's

Code". RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The AES candidate RC6 was based on RC5.

- **Registration Authority (RA):** The person in the public key infrastructure (PKI) who verifies network user requests for a digital certificate and tells the certificate authority (CA) to issue it.
- **Rijndael** (pronounced rain-dahl): The algorithm that NIST selected for the Advanced Encryption Standard (AES). Designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, the Rijndael algorithm is symmetric block cipher that supports key sizes of 128, 192, and 256 bits, with data handled in 128-bit blocks. Rijndael uses a variable number of rounds, depending on key/block sizes.
- **Rivest-Shamir-Adleman (RSA):** An asymmetric cryptography algorithm.
- **Robust Security Network (RSN):** See **WPA2**.
- **Root Certificate:** The final certificate in a chain of verified certificates.
- **Root Certification Authority:** The owner of the root certificate who is trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.
- **S/Key:** A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords from remote user login. The client generates a one-time password by applying the Message-Digest cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.
- **Secure Data Transfer (SDT):** An IRS approved process for exchanging data with trading partners. SDT provides encrypted electronic transmission of IRS files with state and municipal tax agencies electronically over the Internet. IRS has chosen Tumbleweed's (purchased by Sopra Group) SecureTransport product for SDT.
- **Secure Hash Algorithm (SHA):** The most widely-used hash function, called SHA-1, was developed by NIST, to be used with the Digital Signature Algorithm, and was published in 1995 as FIPS 180-1.
- **Secure Hash Standard (SHS):** Specification for a secure hash algorithm that can generate a condensed message representation called a message digest.

- **Secure Shell (SSH):** A network protocol that establishes an encrypted tunnel between a SSH client and a server, as well as authentication services. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary. It is frequently used for remote server administration (log in, execute commands, move files), but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections; it can transfer files using the associated Secure FTP or Secure Copy (SCP) protocols. SSH uses the client-server protocol. An SSH server, by default, listens on the standard TCP port 22.
- **Secure Sockets Layer (SSL):** A protocol for transmitting private documents via the Internet that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. By convention, websites (URLs) that require an SSL connection start with “*https:*” instead of “*http:*”.
- **Secure Multipurpose Internet Mail Extension (S/MIME):** A widely used standard for encrypting and digitally signing e-mail.
- **Security Assurance Requirement (SAR):** A description of the measures taken during development and evaluation of an IT security product to assure compliance with the claimed functionality.
- **Sensitive Information:** An optional, State Entity-defined data classification category that describes information that requires additional levels of protection, but that does not meet the threshold for classification as confidential and may be subject to disclosure or release under the Public Information Act. Examples of data that may not be confidential, but may require additional protections due to state entity-defined proprietary, ethical, operational, or privacy considerations include: contractual data, intellectual property, commercial negotiations, security procedures, or salary information. Note: Sensitive information may also be identified as: controlled, limited access, private, privileged, protected, or restricted information.
- **Session Key:** A symmetric encryption key that is temporary or is used for a relatively short period of time. Usually used for a defined period of communications between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and needs to be re-keyed frequently.
- **Shadow Password Files:** A system file in which encryption user passwords are stored to ensure that are not available to people who try to break into the system.

- **Signature Certificate:** A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
- **Signing Key Pair:** A pair of keys consisting of a private key for signing and a public key for signature verification.
- **Single Point Keying:** A means of distributing keys to multiple, local crypto-equipment or devices from a single fill point.
- **Start-up KEK:** A Key-encryption-Key held in common by a group of potential communicating entities and used to establish ad hoc tactical networks.
- **Stream Cipher:** Methodology that encrypts a single bit, byte, or computer word at a time.
- **Symmetric Encryption (Cryptosystem):** A method of encryption in which the same key is used for both encryption and decryption of the data. The sender uses the key and algorithm to encrypt, and the receiver uses both to decrypt. Both sender and receiver must possess the key, which must remain private.
- **Symmetric Key:** An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret or private. Symmetric key algorithms in common use are designed to have security equal to their key length.
- **Synchronous Crypt-operation:** Method of on-line crypto-operations in which crypto-equipment and associated terminals have timing systems to keep them in step.
- **Temporal Key Integrity Protocol (TKIP – tee-kip):** A cipher suite for enhancing the WEP protocol that the Wi-Fi Alliance endorsed under the name Wi-Fi Protected Access (WPA). TKIP is a wrapper that goes around the existing WEP encryption; it comprises the same encryption engine and RC4 algorithm defined for WEP. However, the key used for encryption in TKIP is 128 bits long. TKIP enables increased security without requiring hardware replacement. TKIP uses three distinct keys: two integrity keys and an encryption key and provides confidentiality protection and integrity protection (through generation of a message integrity code [MIC]) for IEEE 802.11 WLANs:
- **Token:** A device (e.g., floppy disk, Common Access Card, smart card, PC Card, or Universal Serial Bus device) that protects and transports the private keys of a user.

- **Traffic Encryption Key (TEK):** The key used to encrypt plain text (or super encrypt) previously encrypted text and/or to decrypt cipher text.
- **Transport Layer Security (TLS):** A protocol that ensures privacy between communicating applications and their users on the Internet. TLS uses asymmetric encryption for authentication, and symmetric encryption to protect the remainder of the communications session. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS can be used to secure transactions, e-mail, telnet, and FTP sessions. A wireless version of TLS is called WTLS, (wireless transaction layer security). TLS is the successor the SSL.
- **Triple Data Encryption Algorithm (TDEA) or Triple DES (3DES):** A FIPS-approved block cipher, based on DES, that transforms each 64-bit plain text block by applying the Data Encryption algorithm three successive times, using either two or three different keys. 3DES has a key size of 168 bits that provides an effective key length of 112 bits of security, since an attack of complexity 2^{112} is known. Triple DES results in higher processing overhead. [NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004].
- **Triple DES (3DES):** See **Triple Data Encryption Algorithm (TDEA)**.
- **Triple-Wrapped. S/MIME:** Data that has been signed with a digital signature, then encrypted, and then signed again.
- **Trusted Certificate (or Trust Anchor):** A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a
- **Trusted Platform Module (TPM):** A hardware security device that is included in a computer's motherboard chipset and that facilitates the secure creation and storage of cryptographic keys and controls key access.
- **Tunneled Transport Layer Security (TTLS):** A wireless security protocol, similar to PEAP that uses TLS encryption and doesn't require the WLAN clients to have digital certificates. Certificates are stored on the server only, while clients use passwords or tokens for authentication. Often implemented in an environment that does not have a working PKI structure. Unlike PEAP, TTLS supports other EAP authentication methods and also PAP, CHAP, MS-CHAP and MS-CHAPv2, whereas PEAP can tunnel only EAP-type protocols.
- **Tweaked Codebook mode (TCB):** See XTS

- **Tweak Value:** The 128-bit value used to represent the logical position of the data being encrypted or decrypted with XTS-AES.
- **Twofish:** A 128-bit symmetric block cipher with a variable length key (128, 192, or 256-bit). It was one of the five finalists of the AES contest, but was not selected. It is related to the earlier Blowfish block cipher and is unpatented freeware.
- **Virtual Private Network (VPN):** Protected information system link utilizing tunneling, security controls, and end-point address translation giving the user the impression a dedicated line exists between nodes.
- **Virtual Private Network (VPN) Gateway:** An encrypted tunnel between a remote external gateway and the internal network. Placing VPN capability on the firewall and the remote gateway protects information from disclosure between the gateways but not from the gateway to the terminating machines. Placement on the firewall, however, allows the firewall to inspect the traffic and perform access control, logging, and malicious code scanning
- **Virtual Private Network (VPN), Firewall-based:** A firewall-based VPN implementation creates an encrypted tunnel between firewall devices. The extra processing load on the firewalls makes this a slower data transfer rate, but it is generally more secure and easier to administer than hardware VPNs.
- **Virtual Private Network (VPN), Hardware-based:** A hardware-based VPN typically consists of specially designed and dedicated devices that offer hardware and software to terminate encrypted tunnels from one corporate network to another. There is very little processing other than encryption the packet and attaching the TCP/IP headers, creating very fast data transfer, but the infrastructure cost is relatively high.
- **Virtual Private Network (VPN), Software-based:** A software-based VPN is usually the slowest, but most flexible VPN implementation, typically installed on home computers where there may not be any dedicated router or firewall devices.
- **Volume Encryption:** See **Full Volume Encryption (FVE)**.
- **Whole Disk Encryption:** See **Full disk encryption (FDE)**.
- **Wireless Fidelity (Wi-Fi):** A popular wireless technology used in home networks, mobile phones, video games and more.
- **Wi-Fi Protected Access (WPA and WPA2):** A certification program to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. This protocol was created in response

to serious weaknesses in WEP. The WPA protocol implements the majority of the IEEE 802.11i standards. WPA2 is also called **RSN** (Robust Security Network).

- **Wired Equivalent Privacy (WEP):** A limited security protocol for wireless LANs defined in the IEEE 802.11b standard.
- **Wired Equivalent Privacy (WEP) Key:** A series of characters (either a password composed of letters, digits, and punctuation, or a long hexadecimal number) that is used to limit access to a wireless network.
- **Xor-Encrypt-Xor (XEX):** A tweakable encryption mode designed to allow very efficient processing of consecutive blocks.
- **XTS-AES algorithm (or XTS, XEX-based Tweaked Codebook mode (TCB) with CipherText Stealing (CTS), XEX-TCB-CTS):** A mode of operation of AES with tweak and ciphertext stealing for encryption of sector-based storage. Although logically abbreviated as XTC, the “C” was replaced with “S” (for “stealing”) to avoid confusion with ecstasy, an illegal drug. Ciphertext stealing provides support for sectors with size not divisible by block size. XTS acts on data units of 128 bits or more and uses the AES block cipher as a subroutine. XTS addresses threats such as copy-and-paste attack, while allowing parallelization and pipelining in cipher implementations. XTS is supported by dm-crypt, FreeOTFE and TrueCrypt disk encryption software. [See: IEEE P1619 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, Dec 2007.]
- **Zeroization:** A method of erasing electronically stored data, cryptographic keys, and critical stored parameters by altering or deleting the contents of the data storage to prevent recovery of the data.

2. ENCRYPTION POLICY

2.1 Encryption Strength

Based on the risk assessment described above, HSC uses technology(ies) for encrypting confidential data . Symmetric cryptosystem key lengths should be at least 80 bits for confidential data. Asymmetric cryptosystem keys must be of a length that yields equivalent strength, (e.g., approximate equivalencies of 64 bit symmetric = 512 bit asymmetric; 80 bit = 1024 bit; 112 bit = 2048 bit; 128 bit = 3072 bit).

- All encryption mechanisms implemented to comply with this policy support a minimum of, but not limited to, the industry standard.
- The use of proprietary encryption algorithms are not allowed for any

purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the HSC ISO.

- HSC's key length requirements will be reviewed annually and upgraded as technology allows.

2.2 Data at Rest

Hard drives that are not fully encrypted, (e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices), may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.

- Confidential information at rest on computer systems owned by and located within HSC controlled spaces and networks should be protected by at least one of the following:
 - Encryption, or
 - Firewalls with strict access controls that authenticate the identity of those individuals accessing the specific data, or
 - Sanitizing the data requiring protection during storage to prevent unauthorized exposure (e.g., truncating last four digits of a primary account number), or
 - Other compensating controls including: complex passwords, physical isolation/access.
- Password protection should be used in combination with all controls including encryption. Password protection alone is not an acceptable alternative to protecting confidential information.
- Computer hard drives or other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure in accordance with TAC §202.78, Removal of Data from Data Processing Equipment.

2.3 Portable Computing Devices

Portable computing devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential information are the result of stolen or lost portable computing devices. The best way to prevent these exposures is to avoid storing confidential information on these devices. As a general practice, confidential information should not be copied to or stored on a portable computing device or a non-HSC owned computing device. However, in situations that require confidential information to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

- Each designated information resource owner will identify information that is confidential.
- The information resource owner and ISO will specify practices to include written authorization that verifies a legitimate business need for accessing and storing confidential information on a portable device and assesses the risk of unauthorized access to or loss of the data before granting permission for exceptions to this best practice.
- All users must obtain specific permission from the data owner before storing confidential data on a portable computing device or a non-HSC owned computing device.
- Confidential information stored on portable computing devices must be encrypted using products and/or methods approved by the HSC (ISO) (such as full disk encryption with pre-boot authentication).
- Portable computing devices including cell phones should not be used for the long-term storage of any confidential information.
- Portable computing devices including those that store or transmit confidential information must have the proper protection mechanisms installed. This includes unnecessary services and ports turned off and necessary applications being properly configured.
- Removable media that contain confidential information must be encrypted and stored in a secure, locked location.
- Removable media that contain confidential information must be transported in a secure manner.
- Portable or removable media that contain confidential information must be in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).
- The receiver of the removable media must be identified to ensure the person requesting the data is the one claimed.
- HSC OIT will inventory encrypted devices and validate implementation of encryption products at least annually.
- Data owners and users of portable computing devices and non-HSC owned computing devices containing confidential information must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the owner in the event that an

encryption key becomes lost or forgotten. Methods to meet this requirement include:

- Maintaining an accessible copy of the data on a server managed by the HSC, using procedures specified by the HSC.
- Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
- Escrowing the encryption key with a trusted party designated by the data owner and the HSC ISO.

2.4 Transmission Security

Users will follow HSC Internal Policy 29.01.99.Z1.01 Acceptable Use of Information Resources when transmitting data and must take particular care when transmitting or re-transmitting confidential information (e.g., citizen personal identification information) received from non-state employees.

- Confidential information transmitted as an email message must be encrypted.
- Any confidential information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with HSC must be encrypted or be transmitted through an encrypted tunnel.
- Transmitting unencrypted confidential information through the use of web email programs is not allowed.
- The download or installation of any Instant Messaging (IM) or online peer-to-peer (P2P) file sharing programs requires specific authorization in writing from the IRM. All approved HSC P2P or IM networks will use tools that encrypt the traffic flows between peers and only allow access to a managed IM server which provides gateways to public services.
- Wireless (Wi-Fi) transmissions that are used to access HSC portable computing devices or internal networks must be encrypted using WPA2 enterprise standard or better.
- Encryption is required when users access HSC data remotely from a shared network, including connections from a Bluetooth device to a HSC PDA or cell phone.
- HSC permits the secure encrypted transfer of documents and data over the Internet using file transfer programs such as “Secure FTP” (FTP over SSH) and SCP. Only authorized HSC users can initiate Secure FTP or SCP transactions and will use the following procedures:
 - To use the transmitting server securely, each authorized user must

have a logon ID and password with a designated directory. Users should not have access to shared directories unless required for business reasons. Anonymous FTP is not permitted.

- All accounts and keys must be managed from within HSC's network.
- All transactions and transfers must be logged, and reviewed for prohibited activity.
- All files contained within an account's directory must be deleted seven days after they are delivered or made available for retrieval.
- Plain FTP does not provide encrypted transmission and should not be used on any Internet-facing systems or where confidential information is being transmitted.

2.5 Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements. HSC key management systems are characterized by the following security precautions:

- HSC uses procedural controls to enforce the concepts of least privilege and separation of duties for personnel (per National Institute of Standards and Technology Special Publication 800-53 guidelines). These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor personnel. The ISO will verify backup storage for key passwords, files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.
 - No single individual is authorized to generate a new CA key pair.
 - Regular audit trail reviews are conducted.
 - The HSC OIT will verify the subject's identity.
 - Background checks and clearance procedures required for the personnel.
 - Complete regular training on key management requirements and procedures.
 - Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of HSC systems.
 - Written acknowledgement of receipt of this policy from each individual involved in key management.
- Keys in storage and transit must be encrypted.
- Private keys must be kept confidential.

- Keys must be randomly chosen from the entire key space, using hardware-based randomization.
- Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key (e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure).
- HSC uses short key life or crypto-periods with defined activation and deactivation duration limits; for the following key types with maximum crypto-periods for originators and recipients as indicated below. Originator Usage Periods (OUP) are differentiated from Recipient Usage Periods when applicable.
- Keys with a longer life are sparsely used and must be approved by the ISO. The key shall be destroyed at the end of its crypto-period. (The cost of changing keys rises linearly while the cost of attacking the keys rises exponentially. Therefore, all other factors being equal, changing keys will increase the effective key length of an algorithm.)
- Keys that are transmitted are sent securely to well-authenticated parties.
- Key-generating equipment is physically and logically secure from construction through receipt, installation, operation, and removal from service.

The HSC key management system or vendor will provide written security policies and procedures that address encryption key:

- Generation processes for different cryptographic systems and different applications.
- Distribution, access, and activation for authorized users.
- Storage, archiving, and destruction.
- Changes and updates, including rules on when keys should be changed and how this will be done.
- Compromises or loss of control incidents.
- Revocation with specific withdrawal or deactivation procedures.
- Recovery when lost or corrupted as part of business continuity planning.

- Roles, responsibilities, facilities, and procedures for all organizational elements to reliably recover critical data.
 - Specification of circumstances and process for authorizing key recovery.
 - Generation (e.g., whether or not the material was centrally-generated).
 - Storage and access for long-term storage keys.
 - Process of transitioning from the current to future long-term storage keys.
- Audit logging of management-related activities.
 - Activation and deactivation dates and usage period limits.

3. DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY

Vice President for Information Technology and Chief Information Officer