


| | | |
|---|--|--------------------------------|
|  | Information Security Policies and Procedures | No. COMP-Sec 8.1.3 |
| | Title: ENCRYPTION CONTROL PROCEDURE | Page: 1 of 4 |
| | | Revised Date: 12/22/04 |
| | | Original Date: 01/15/01 |

Encryption Control Procedure

I. SCOPE

This procedure applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This procedure applies to all Tenet information assets and information asset Administrators.

II. PURPOSE

Provide direction for administration of encryption techniques. Tenet shall employ encryption when sending *CONFIDENTIAL* information over un-trusted networks.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

III. PROCEDURE

Information asset administrators shall ensure encryption techniques are applied consistent with approved Tenet Information Security Policies and Procedures.

A. Encryption Methods

The following methods may be used to encrypt information that is transmitted over un-trusted networks.


1. EMAIL ENCRYPTION

Emails transmitted from tenethealth.com (or other Tenet managed domains) addresses to external email accounts can be encrypted by using the secure email solution approved by the Corporate Information Systems Department. This solution encrypts the body and attachments, but not the subject, of the email during transmission.

2. DATA ENCRYPTION

Data may be encrypted for transmission or storage using one of the following methods.

- a) **Proven encryption technologies** that apply standard algorithms (i.e. 3DES,

| | | |
|---|--|--------------------------------|
|  | Information Security Policies and Procedures | No. COMP-Sec 8.1.3 |
| | Title: ENCRYPTION CONTROL PROCEDURE | Page: 2 of 4 |
| | | Revised Date: 12/22/04 |
| | | Original Date: 01/15/01 |

AES, Blowfish, IDEA, RSA, RC5) may be used to protect data files. These algorithms represent the actual cipher used for an approved application (i.e. PGP, GPG, etc). Proprietary algorithms are not considered an acceptable method for securing *CONFIDENTIAL* information. Symmetric cryptosystem key lengths must be at least 128 bits, while asymmetric cryptosystem keys must be of a length that yields equivalent strength.

- b) **WinZip Version 9.0** or higher may be used to encrypt data when proven encryption technologies could not reasonably be applied. The decision to use WinZip instead of proven encryption technologies should be documented in the facility's Information Security Control Exceptions Book.
- c) **Password-protected files** may be used to safeguard data when proven encryption technologies and WinZip 9+ could not reasonably be applied. The decision to use password-protected files (i.e. Excel file with password protection) instead of proven encryption technologies and WinZip 9+ should be documented in the facility's Information Security Control Exceptions Book.


3. HARD DISK ENCRYPTION

The hard disk(s) of information assets may be encrypted using one of the following methods.

- a) **Full disk encryption** technologies that apply standard algorithms (i.e. 3DES, AES) to encrypt the entire hard disk, including the operating system, may be utilized. These solutions should employ pre-boot authentication and provide complete power off protection. Cryptosystem key lengths must be at least 128 bits, but 256 bit encryption or above is recommended.
- b) **Virtual disk encryption** technologies that apply standard algorithms (i.e. 3DES, AES) to encrypt a portion of the hard disk may be utilized where full disk encryption would not be feasible. If virtual disk encryption is employed instead of full disk encryption, special attention should be paid to ensure that the operating system passwords for all users meet the guidelines outlined in Password Use Procedure No. 3.3.2. Cryptosystem key lengths must be at least 128 bits, but 256 bit encryption or above is recommended.

4. WIRELESS ENCRYPTION

Encryption should be enabled for wireless transmissions. The 802.11i standard should be used as the preferred security architecture for wireless, and encryption

| | | |
|---|--|--------------------------------|
|  | Information Security Policies and Procedures | No. COMP-Sec 8.1.3 |
| | Title: ENCRYPTION CONTROL PROCEDURE | Page: 3 of 4 |
| | | Revised Date: 12/22/04 |
| | | Original Date: 01/15/01 |

should be enabled on all such implementations. Where implementation of 802.11i is not feasible, WAP or WEP may be used to provide wireless encryption, preferably together with an application layer Virtual Private Network (IPSEC VPN or SSL VPN). A minimum 128-bit key strength should be implemented, and unique key encryption (per individual) should be implemented instead of shared key (one for everyone) encryption.

B. Digital Certificates


Any Tenet information asset used to access *CONFIDENTIAL* information over the Internet shall use digital certificates to validate the identity of both the User and the server.

- a) Certificates may only be issued by certificate authorities approved by Tenet's Corporate Information Systems Department.
- b) Certificates at the User end shall be employed in conjunction with standard technologies such as Secure Sockets Layer (SSL) to provide continuous authentication to eliminate the risk of session hijacking.
- c) Access to digital certificates stored on personal computers shall be protected by passwords or pass-phrases. All policies for password management shall be followed (See Password Control Procedure No. 8.1.1 for further information).

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0 and its subordinate Standard and Procedures.
- Security Risk Management Standard No. 7.1.0.
- Technical Security Administration Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0.
- Password Control Procedure No. 8.1.2.
- Network Security Administration Procedure No. 8.3.1.

| | | |
|---|--|--------------------------------|
|  | Information Security Policies and Procedures | No. COMP-Sec 8.1.3 |
| | Title: ENCRYPTION CONTROL PROCEDURE | Page: 4 of 4 |
| | | Revised Date: 12/22/04 |
| | | Original Date: 01/15/01 |

- Transmission Security Procedure No. 8.3.6.