Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.33.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A*	*REV. B*
POLICY: **Encryption Standard Policy**	*PAGE 1 OF 3*		

PURPOSE

This standard provides the standard practices that must be followed when using encryption technology. Implementation of this standard ensures the consistent application of the guidelines utilized across all areas of the university, thereby benefiting the users and administrative functions.

The ability to require all users to abide by the same standard for using encryption will help to insure that Creighton information is adequately protected, non-repudiation is maintained and that data recovery is available.

SCOPE

This standard applies to all members of the Creighton community including all temporary and contract workers. It applies to all production computer systems used at Creighton, whether in the delivery of internal services to faculty, staff, and students; or to the delivery of services to external customers.

STANDARD

Creighton University strives to provide the highest level of security for all critical data while balancing the challenge of protecting "data at rest" such as that defined in the Access Control standard of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule against the increase in security technology complexity and administrative overhead including performance considerations and usability.

Creighton University will seriously review the viability of securing critical database, file servers as well as ePHI on mobile devices such as laptops and PDAs.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application

Symmetric cryptosystem key lengths must be at least 56 bits.

Asymmetric crypto-system keys must be of a length that yields equivalent strength.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer.

Creighton University will test encryption and decryption capabilities of products and systems to ensure proper functionality.

File Encryption

There were several requirements that the encryption solution had to meet in order to be approved for use within Creighton. These requirements include file level encryption and decryption, secure file delete, integration into the desktop and applications, friendly user interface, key recovery, support for several encryption algorithms and key strengths, with technology based on the industry standards.

E-Mail Encryption
Creighton is currently evaluating secure email solutions. In the meantime email should be viewed as insecure medium therefore confidential information should not be sent via email.

World Wide Web Traffic Encryption
The Secure Sockets Layer (SSL) protocol using 128-bit key lengths has been approved for use to encrypt web traffic.

Remote Access
The University approved method of remote access is based on VPN technology which forces all traffic through an encrypted tunnel. Therefore, all remote access traffic passed between the Creighton network and the end users is fully encrypted.

Password Encryption
Creighton's policies do not allow passwords to be sent across the network in 'clear text' format. Passwords must also not be listed in clear text for the purpose of automating a login sequence. All passwords must be stored and transmitted in an encrypted format by the OS, DBMS, or application.

DEFINITIONS

Cryptography
The art and science of keeping messages secure. In addition to offering confidentiality, cryptography is used to provide authentication, integrity, and non-repudiation.

Clear Text
Non-encrypted data

Non-repudiation
After you do it, you can't say you didn't

128-bit encryption
Encryption key that is 128 bits in length

SSL
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses the public-and-private key encryption system, which also includes the use of a digital certificate.

Digital Certificate
A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real

RESPONSIBILITIES

Information Security is responsible for evaluating and approving new encryption technologies and software, as well as reviewing and approving all requests to use cryptographic technology within Creighton. The Information Security Department is also responsible for maintaining and updating this standard as necessary.

Systems Administrators are responsible for obtaining and installing server side digital certificates that are used for server authentication in SSL transactions.

Network Users are responsible for adhering to the Cryptography Policy and Encryption Standard when handling Confidential Creighton University information.

REFERENCES TO APPLICABLE STANDARDS

HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/, February 20, 2003.

EXCEPTIONS

None

VIOLATIONS/ENFORCEMENT

Any known violations of this standard should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this standard can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University policies.

The University may advise law enforcement agencies when a criminal offense may have been committed.