Adminstrative Policies

College Encryption and Key Management Standard

The following standard is under the jurisdiction of the College's Information Security (ISec) Committee and maintained by the Office of Computer and Information Systems

Encryption

All encryption methodologies and products must be approved by the College ISec Committee and must include the following:

A. Encryption products must have Federal Information Processing Standard (FIPS) 140 (Security Requirements for Cryptographic Modules) validation.

B. Full disk encryption products must utilize pre-boot authentication.

C. The Office of Computer and Information Systems must inventory encrypted devices and media and validate that the encryption product has been successfully implemented.

Key Management

Cryptographic keys used to encrypt and decrypt information must be protected in a secured environment. Keys must be securely distributed and stored. Access to these keys is restricted to only those individuals who have a business need to access the keys. Information encrypted with a key that has been compromised is no longer to be considered encrypted and must be re-encrypted as soon as possible. The following procedures must also be followed:

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

B. Keys must be protected with a password that conforms to the College's minimum Password Standard.

C. Compromise of a key will require that a new key be generated to continue protection of the encrypted information.

D. Encryption keys and software products must be maintained for the life of encrypted archived data.

Approved by Executive Council
February 12, 2010