

Information and Technology Services Standards

Procedure Name: Campus Encryption Standard	Temporary Review Number:
Classification: Information Technology Services	Supersedes:
Author: Kevin Thompson	Last Review:
Authority:	Next Review:
Application: All University	Effective Date:
Distribution: All University	Custodian of Policy: ITS

STANDARD:

Acceptable encryption algorithms for government data are outlined in the Federal Information Processing Standard 140-2 (Security Requirements for Cryptographic Modules). Encryption products must be validated by the Nation Institute of Standards and Technology as complying with FIPS Publication 140-2 at any level. Approved standards for encryption, hashing, digital signatures, random number generating, and message authentication include: AES, 3DES, Skipjack, DSA, RSA, SHA, CMAC, CCM, HMAC, and MAC.

The use of an encryption algorithm that is not on the government list will be considered acceptable if the algorithm is a published, open standard that has withstood at least three years of peer review. Additionally, the encryption algorithms used by FileVault and Bitlocker is considered acceptable for protecting government data.

Data Encryption Standard (DES) is not considered sufficient protection for sensitive information unless no other alternative is available. Additionally, the use of proprietary encryption algorithms or “home grown” encryption algorithms that were developed in house or algorithms that have not been subjected to substantial peer review are not considered acceptable for protecting sensitive information.

RECOMMENDED PRODUCTS:

WHOLE DISK ENCRYPTION	OPERATING SYSTEM
Pointsec for PC with AES Encryption	Microsoft Windows XP, 2000, & Vista
Bitlocker	Microsoft Vista
FileVault	Mac OS X
Pointsec for Linux	Linux
LUKS with AES	Linux

DATA AT REST	OPERATING SYSTEM
PGP/GPG	Microsoft Windows, Mac OSX, linux
TrueCrypt	Microsoft Windows, linux
Loopback Encrypted File System with AES	Linux
Pointsec Media Encryption	Microsoft Windows XP, 2000

DATA IN MOTION	OPERATING SYSTEM
SSH	All
SSL/TLS	All
IPSEC or SSL VPN	All

AUTHORITY:

MnSCU Board Policy 5.23: Security and Privacy of Information Resources

<http://www.mnscu.edu/board/policy/523.html>

Minnesota State University, Mankato Campus Information Privacy Policy

<http://www.mnsu.edu/policies/privacy.pdf>

SEE ALSO:

Security Requirements for Cryptographic Modules (FIPS Publication 140-2)

<http://csrc.nist.gov/cryptval/>

Validated FIPS 140-1 and 140-2 Cryptographic Modules

<http://csrc.nist.gov/cryptval/140-1/140val-all.htm>