Guideline 5.23.1.2 Encryption for Mobile Computing and Storage Devices

Part 1. Purpose: With advances in computer technology, mobile computing and storage devices (mobile devices) have become useful tools to meet the business needs within Minnesota State Colleges and Universities (system). However, these mobile devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. Encryption is one part of an asset protection strategy to ensure the availability and integrity of system information resources. Additional steps may be appropriate to protect from theft or loss any mobile device that may transmit and/or store system information resources regardless of ownership of such devices.

Part 2. Applicability: Where encryption is required by system policy or procedure, this guideline states general principles and currently acceptable and unacceptable encryption methods for mobile devices that transmit and/or store system information resources. As technology changes, this guideline will be amended to reflect improved encryption methodology. Institutions may adopt additional security practices for information technology resources under their control consistent with this guideline and other applicable system policies and procedures including, but not limited to, Board policy 5.23. Minnesota State Colleges and Universities is not responsible for any personal or unauthorized use of its resources, and security of data transmitted on its information technology resources cannot be guaranteed.

Part 3. Guidelines:

Subpart A. Current acceptable methods of encryption include[1], but are not limited to:

1. AES, where the key length must be 128 bits or higher.
2. RSA, where the key length must be 3,072 bits or higher.

Subpart B. Once NIST has determined that an encryption method is found to be unacceptable, it is considered unacceptable for use within the system. Current unacceptable encryption methods include, but are not limited to:

1. DES at a 56 bit key length.
2. RC4.

Subpart C. Encryption can be applied to a whole disk, a folder, or at the file level.

[1] See FIPS 140-2 *Security Requirements for Cryptographic Modules* and NIST *Cryptographic Module Validation Program* for a list of certified encryption products (which generally advertise themselves as certified) and algorithms, including key length recommendations.

Subpart D. Key Recovery.

1. To ensure availability, when an unencrypted copy of the data is not maintained, encryption techniques and methods must provide key recovery capabilities.
2. Key recovery functionality must provide for recovery of user encryption keys for the life of the data by the Authorized system or Institutional Official.

Part 4. Definitions:

Subpart A. Advanced Encryption Standard (AES). A current encryption algorithm commonly used in symmetric key cryptography.

Subpart B. Authorized System or Institutional Official. The person designated by the Chancellor, Director or Department Head to function in an authorization role for information/data access purposes. In some cases, the employee's supervisor may function as the designee. In other cases, a key contact is named

Subpart C. Availability. The accessibility of data or information to authorized users when needed.

Subpart D. Data. Information collected, stored, transferred or reported for any purpose, whether in computers or in manual files. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value, and because it has various sensitivity classifications defined by Federal law and State Statute, it must be protected.

Subpart E. Data Encryption Standard (DES). An outdated encryption algorithm used in symmetric key cryptography.

Subpart F. Encryption. The process of transforming information/data to make it unreadable to anyone except those authorized, possessing special knowledge, which is typically referred to as the key. The transformation process results in encrypted information/data.

Subpart G. Federal Information Processing Standards (FIPS). Publicly announced standards developed by the United States Federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.).

Subpart H. Institution. A system college or university, the system office, or the Minnesota State Colleges and Universities system.

Subpart I. Integrity. The protection of information to assure it is kept intact and not lost, damaged, or modified without proper authorization.

Subpart J. May. A statement that is optional.

Subpart K. Minnesota Government Data Practices Act (MGDPA). Per Minnesota State Statute §13, MGDPA regulates the collection, creation, maintenance and dissemination of government data in state agencies, statewide systems, and political subdivisions. It establishes a presumption that government data are public and are accessible by the public

for both inspection and copying unless there is a federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

Subpart L. Mobile Computing Devices. The term "mobile computing devices" refers to portable or mobile computing and telecommunications devices that can execute programs. This definition includes, but is not limited to, notebooks, palmtops, PDAs, IPods, BlackBerry devices, and cell phones with internet browsing capability.

Subpart M. Mobile Storage Devices. The term "mobile storage devices" includes but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

Subpart N. Must. A statement that is required for a compliant implementation.

Subpart O. Must Not. A statement that is prohibited for a compliant implementation.

Subpart P. National Institute of Standards and Technology (NIST). A measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

Subpart Q. Not Public data. Data that is considered confidential, private, nonpublic or protected nonpublic data as defined in the MGDPA or any other relevant state or federal statute or system legal guideline. For examples of data classifications, see standard 5.23.E, Notice of Breach of Security, Part 4: Reporting a Suspected Breach.

Subpart R. Rivest Cipher [version] 4 (RC4). An outdated stream cipher encryption algorithm.

Subpart S. Rivest Shamir Adleman (RSA). A current encryption algorithm commonly used in asymmetric public-key cryptography.

Subpart T. Should. A statement that is recommended but not required.

Subpart U. Should Not. A statement of practices that are not recommended but which may be followed.

Subpart V. System. Referring to the Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Subpart W. User. Any individual, including but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using system information resources, whether or not the user is affiliated with the system.

Part 5. Authority.

Subpart A. Board policies 1A.1 and 5.23 delegate authority to the vice chancellor to develop system guidelines, consistent with Board policy and system procedure, for the purposes of implementing Board policy 5.23.

Approval Date: 02/09/09,
Effective Date: 03/09/09,

Date and Subject of Revision:

1/25/12 – The Chancellor amends all current system procedures effective February 15, 2012, to change the term "Office of the Chancellor" to "system office" or similar term reflecting the grammatical context of the sentence.