

Information Services & Technology Acceptable Encryption Policy

I. PURPOSE

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

II. APPLICABILITY

This policy applies to all UMDNJ employees, students and affiliates.

III. ACCOUNTABILITY

Under the President, the Senior Vice Presidents shall ensure compliance with this policy. The Vice President for Information Systems and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

IV. DEFINITIONS

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

V. POLICY

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. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. DES 56 bit encryption may be used for transient less sensitive data. For all other data a minimum of 128 bit key length is required. Asymmetric crypto-system keys must be of a length that yields equivalent strength. UMDNJ's key length requirements will be reviewed annually and upgraded as technology allows.

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 IS&T. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the

United States should make themselves aware of the encryption technology laws of the country in which they reside.

VI. NON-COMPLIANCE AND SANCTIONS

Any person found to have violated this policy may be subject to denial or removal of access privileges to the University network; disciplinary action under applicable University policies and procedures up to and including termination; civil litigation; and/or civil or criminal prosecution under applicable state and federal statutes.