



Chapter Name

8.0 SECURITY

Chapter Number

Title

8.2

Acceptable Encryption Policy

1.0 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.

2.0 Scope

This policy applies to all persons communicating with, working for, resident in or affiliated with Eastern Michigan University, or other persons using, holding, or storing University data or any other person's personal data controlled by the University.

3.0 Policy

The use of encryption algorithms is restricted to those explicitly approved in current ICT standards. Specific examples of algorithms listed in this policy are not necessarily approved.

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-Hellman, while Secure Socket Layer (SSL) uses RSA encryption.

Symmetric cryptosystem key lengths must meet minimum qualifications listed in current ICT standards. Asymmetric crypto-system keys must be of a length that yields equivalent strength. EMU'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 Network Engineering Team and Director of IT Security Administration. 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.

4.0 Responsibility for Implementation

Director of IT Security Administration and Director IT, Network and Systems.

5.0 Enforcement

Any user found to have violated this policy may be subject to loss of certain privileges or services, and other disciplinary actions or legal sanctions, civil and criminal.

6.0 Definitions	
<u>Term</u>	<u>Definition</u>
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).
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.

7.0 Revision History			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
ICT Security	Modeled after SANS Institute Policy		
ICT Security	ICT Security Team	May 17, 2005	
Barr	Revised	June 19, 2005	
French	Revised	June 21, 2005	
Popp	Submitted to CIO	July 28, 2005	September 1, 2005
Laundra	Copyedited/Proofed for Upload	September 1, 2005	