



Cyber Tree Systems

A Business IT Solution Company

POLICY NAME	Acceptable Encryption		
DATE OF LAST REVISION:	9/4/2003	VERSION NO.	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public reviews 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.

Scope

This policy applies to all CTS employees and affiliates.

Policy Statement

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 be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. CTS'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 InfoSec. 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.

Enforcement

Any employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

Terms and Definitions

Define any acronyms, jargon, or terms that might have multiple meanings.

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
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).

Revision History

Revisions made 9/4/2023