SAMPLE POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

POLICY OWNER: Individual responsible for execution or oversight of the policy

EFFECTIVE DATE: Date

Summary

It is the policy of Name of Enterprise to limit the use of cryptographic modules, algorithms, primitives, keys, applications and any associated artifacts only to those that have proven to be resilient against known attacks and that are of sufficient strength to protect assets of Name of Enterprise. This policy specifically requires components that have received public review, that have withstood public and open examination, and that have been vetted by Name of Enterprise personnel and deemed reliable and robust.

This policy further requires that any applicable governing regulation, contractual requirement or other standard will be followed with respect to cryptography, that use of cryptography is appropriate and legal if algorithms or encrypted data may be disseminated outside the United States, and that due diligence is exercised in the use of encryption technology.

Scope

This policy applies to all Name of Enterprise employees, affiliates, subsidiaries, contractors, and other personnel or entities subject to the policy and requirements of Name of Enterprise .

Policy Statement

To be considered approved for use by Name of Enterprise , algorithms, implementations (e.g., software modules or libraries), software or other cryptographic components must appear on the Approved Cryptosystem List, available from the Name of Enterprise security team. Modules that are certified to comply with Federal Information Processing Standard (FIPS) 140 (at level 2 for software modules or level 3 for hardware modules) are considered preapproved for use provided that cryptographic algorithms and parameters approved by the US National Institute of Standards and Technology (NIST) are employed and the modules are configured in NIST mode.

Approved ciphers include AES 256, SHA-256 and RSA employing keys of at least 2048 bits or greater. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of sufficient length to yield equivalent strength. These key-length requirements will be reviewed annually. Proprietary or internally developed encryption algorithms will not be used.

The export of encryption technologies or encrypted data may be restricted by Country regulation. Personnel will seek guidance from the legal department of Name of Enterprise should export of cryptographic technologies or encrypted data be required.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

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)
Federal Information Processing Standard (FIPS)	Standards issued by the US National Institute of Standards and Technology (NIST) to protect sensitive information
NIST	Acronym for the US National Institute of Standards and Technology. NIST is a nonregulatory federal agency within the US Department of Commerce.

Revision History

DATE OF CHANGE	RESPONSIBLE	SUMMARY OF CHANGE

Signature

NAME: _____ **DATE:** _____

Your signature certifies that you have read and understood this policy.