Acceptable Encryption Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

1. Overview

An acceptable encryption policy is a set of guidelines and procedures that an organization follows to ensure that sensitive information is protected using encryption technologies.

2. 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.

3. Scope

This policy applies to all **<Company Name>** employees and affiliates.

4. Policy

4.1 Algorithm Requirements

4.1.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

4.1.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to the date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

4.1.3 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Consider RFC6090 to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing is required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4.2 Hash Function Requirements

In general, **<Company Name>** adheres to the NIST Policy on Hash Functions.

4.3 Key Agreement and Authentication

4.3.1 Key exchanges must use one of the following cryptographic protocols: DiffieHellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

4.3.2 Endpoints must be authenticated prior to the exchange or derivation of session keys.

4.3.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed messages or manual verification of the public key hash.

4.3.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

4.3.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

4.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.4.2 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1 Compliance Measurement: The infosec team will use a variety of techniques, including but not limited to routine walkthroughs, business tool reports, internal and external audits, and reporting to the policy owner, to ensure that this policy is being followed.

5.2 Exceptions: The Infosec team must beforehand approve any exception to the policy.

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

6. Related Standards, Policies, and Processes

National Institute of Standards and Technology (NIST) publication FIPS 140-2, NIST Policy on Hash Functions

7. Revision History

Version	Date	Description
1.0	14-03-2023	Initial Policy