Acceptable Encryption Policy

1. Overview

Encryption is essential for the appropriate protection of sensitive and protected company documents, data and communications. This Acceptable Encryption Policy sets out clear guidelines and requirements on encryption within NIAB.

2. Purpose

The purpose of this policy is to provide rules and guidance on the use of encryption, and specifically outline the algorithms that are acceptable for use within NIAB. These algorithms have received substantial public review and have been proven to work effectively.

3. Scope

This policy applies to all employees, temporary workers, contractors and agents acting on behalf of the company that may use or require knowledge of encryption technologies within their assigned job roles.

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 use of 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 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

4.1.3.1. ECDSA. This algorithm should be used with a minimum key length of P-256.

4.1.3.1. RSA. This algorithm should be used with a minimum key length of 2048. This algorithm must only be used with a secure padding scheme.

4.1.3.2. LWDM. This algorithm should be used with SHA256 encryption.

4.2. Hash Function Requirements

4.2.1. The Company 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. End points 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 message 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).

5. Compliance

5.1. Compliance Measurement

The IT team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. Exceptions

Any exceptions to this policy must be approved by the Infosec team in advance and have a written record.

5.3. Non-Compliance

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