1. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms (problem-solving operations) that have received substantial public review and have proven to work effectively.

2. Scope

This policy applies to all Kinyo employees and affiliates.

3. Policy

3.1 Key derivation Requirements according to RFC2898

3.1.1 The encryption algorithm is based on the Advanced Encryption Standard (AES), the next-generation encryption standard chosen by the U.S. governments National Institute of Standard and Technology (NIST) publications FIPS 140-2, The use of the Advanced Encryption Standards (AES) is strongly recommended for symmetric encryption.

3.1.2 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
PKCS 5	P-256	Consider RFC2898 to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS padding scheme is recommended. Message hashing required.

3.2 Hash Functions Requirements

In general, Kinyo adheres to the NIST Policy on Hash Functions.

3.3 Key Agreement and Authentication

3.3.2 End points must be authenticated prior to the exchange or derivation of sessions keys.

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

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

3.4 Key Generation

3.4.1 based on PKCS password-based cryptography specification version 2.0 by RFC2898, the derived key and initialization vector after 1,000 iterations of password-based key derivation mixed with random numbers as salt are output one after another, and each is used as the key and initialization vector for encryption.

4. Policy Compliance

4.1 Compliance Measurement

The I.T. team will verify compliance to this policy through various methods, including but not limit to, business tool reports, internal and external audits, and feedback to the I.T. department.

4.2 Exceptions

Any exceptions to the policy must be approved by the I.T. team in advance.