P.O. Box 6082, Willemstad, Curaçao – Telephone: +1 (631) 480 2118 (USA) / +599 9 523 2685 (Curacao)

Electronic Encryption Policy

Document version: 01-2023

1 – 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 national and international regulations are followed and legal authority is granted for the dissemination and use of encryption technologies.

2 – Scope

This policy applies to all CUN students, management, faculty, contract staff, freelance staff, providers and affiliates.

3 – Policy

3.1 – Algorithm requirements

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.

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.

Signature Algorithms:

Algorithm	Key Length (min)	Additional Comments
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 required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft.

3.2 – Hash Function requirements

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

3.3 – Key Agreement and Authentication

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

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

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.

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

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

3.4 – Key Generation

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

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

4 – Policy compliance

4.1 – Compliance measurement

CUN appointed officials or third party professionals will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits and feedback to the policy owner.

4.2 – Exceptions

Any third party exception to the policy must be approved by CUN appointed officials in advance.

4.3 – Non-compliance

An employee, contractor or affiliate found to have violated this policy may be subject to disciplinary action.

5 – Related standards, policies and processes

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

6 – Revision History

Date of Change	Responsible	Summary of Change
January 1, 2023		