NATIONAL DATA
MANAGEMENT AUTHORITY

Encryption Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This standard establishes controls for encryption.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

The purpose of this standard is to enhance security and protect electronic data by encryption. Encryption is an effective tool in mitigating the threat of unauthorised access to data.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

The need for encryption of information is based on its classification, risk assessment results, and use case. Attention must be given to the regulations and national restrictions (e.g., export controls) that may apply to the use of cryptographic techniques in different parts of the world.

Encryption products for confidentiality of data at rest and data in transit must incorporate government approved algorithms for data encryption. Hashing algorithms transform a digital message into a short representation for use in digital signatures and other applications to validate the integrity of the message. Although hash functions such as SHA 1, provide a certain amount of security strength, it does not meet all security requirements for keyed-hash functions such as HMAC SHA 1. Of note, SHA-2 and SHA-3 are better alternatives to SHA-1. Refer to FIPS 180-4[1] for more information on different types of application hashing algorithms. Hashing algorithms can be used for multiple purposes including but not limited to, digital signatures, message authentication codes, key derivation functions, pseudo random functions.

Use of outdated, cryptographically broken, proprietary encryption algorithms/hashing functions is prohibited. Electronic information used to authenticate the identity of an individual or process (i.e., PIN, password, passphrase) must be encrypted when stored, transported, or transmitted. This does not include the distribution of a one-time use PIN, password, passphrase, token code, etc., provided it is not distributed along with any other

[1] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center CSRC https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

authentication information (e.g., user-ID). A system's security plan must include documentation to show appropriate review of encryption methodologies and products. This will demonstrate due diligence in choosing a method or product that has received substantial positive review by reputable third-party analysts.

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[2], or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2[3], 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[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

Algorithm	**Key Length (min)**	**Additional Comment**
Elliptic Curve Digital Signature Algorithm (ECDSA)	P-256	Consider RFC6090[4] to avoid patent infringement.
Rivest–Shamir–Adleman (RSA)	2048	Must use a secure padding scheme. PKCS#7 padding scheme[5] is recommended. Message hashing required.
Lamport–Diffie–Winternitz–Merkle (LDWM)	SHA256	Refer to LDWM Hash-based Signatures Draft[6]

4.2 Hash Function Requirements

All government agencies and ministries should adhere to the NIST Policy on Hash Functions[7].

[2] http://tools.ietf.org/html/draft-irtf-cfrg-cipher-catalog-01#section-3.1

[3] https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

[4] https://www.rfc-editor.org/rfc/rfc6090

[5] http://tools.ietf.org/html/rfc3852#section-6.3

[6] http://tools.ietf.org/html/draft-mcgrew-hash-sigs-00

[7] https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions

4.3 Data in Transit

Encryption is required for data in transit in the following situations:

4.3.1 When electronic personally identifiable information (PII) is transmitted (including, but not limited to, e-mail, File Transfer Protocol (FTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).

4.3.2 When encryption of data in transit is prescribed by law or regulation

4.3.3 When connecting to the internal network(s) over a wireless network.

4.3.4 When remotely accessing an entity's internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network. This does not apply to remote access over an entity's managed point to point dedicated connection.

4.3.5 When data is being transmitted with an entity's public facing website and/or web services, they are required to utilise Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP) where technically feasible. Public facing websites must utilise HTTP Strict Transport Security (HSTS), automatically redirecting HTTP requests to HTTPS websites where technically feasible.

Appropriate encryption methods for data in transit include, but are not limited to, Transport Layer Security (TLS) 1.2 or later, Secure Shell (SSH) 2.0 or later, Wi-Fi Protected Access (WPA) version 2 or later (with WiFi Protected Setup (WPS) disabled) and encrypted Virtual Private Networks (VPNs). Components should be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.

4.4 Data at Rest

Encryption is required for data at rest, as follows:

4.4.1 For the systems listed below:

4.4.1.1 desktops that access or contain personally identifying information (PII);

4.4.1.2 data stores (including, but not limited to, databases, file shares) that contain PII;

4.4.1.3 all mobile devices, whether entity issued or third-party, that access or contain any entity information; and

4.4.1.4 all portable storage devices containing any entity information.

4.4.2 When electronic PII is transported or stored outside of the organisation's facility.

Full disk encryption is required for all issued laptops that access or contain organisation information. Full disk encryption products must use either pre-boot authentication that utilises the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.

To mitigate attacks against encryption keys, when outside of the organisation's facilities, laptops and third-party laptops that access or contain PII must be powered down (i.e., shut down or hibernated) when unattended.

The organisation must have a process or procedure in place for confirming devices and media have been successfully encrypted using at least one of the following, listed in preferred order: automated policy enforcement; automated inventory system; or manual record keeping.

4.5 Key Management

The organisation must ensure that a secure environment is established to protect the cryptographic keys used to encrypt and decrypt information. Keys must be securely distributed and stored. Access to keys must be restricted to only individuals who have a business need to access the keys.

Unencrypted keys must not be stored with the data that they encrypt. Keys will be protected with an authentication token that conforms to the identified assurance level. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted. If a compromise has been discovered a new key must be generated and used to continue protection of the encrypted information. Specific circumstances should be evaluated to determine if a breach notification is required. Encryption keys and their associated software products must be maintained for the life of the archived data that was encrypted with that product.

4.6 Key Generation

4.6.1 Cryptographic keys must be generated and stored securely to avoid loss, theft, or compromise.

4.6.2 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[8].

4.7 Key Agreement and Authentication

4.7.1 Exchanges of keys must use one of the following cryptographic protocols: Diffie-Hellman, Internet Key Exchange (IKE), or Elliptic curve Diffie-Hellman (ECDH).

4.7.2 When exchanging or deriving session keys, endpoints must be authenticated.

4.7.3 Public keys used to establish trust must be authenticated before use. Transmission of cryptographically signed messages and manual verification of the public key hash are examples of authentication.

4.7.4 All servers used for authentication (for example, DOMAIN CONTROLLER, RADIUS{Remote Authentication Dial-In User Service}, or TACACS {Terminal Access Controller Access Control System}) must have a valid certificate installed, signed by a well-known and trustworthy authority.

4.7.5 Certificates for all servers and applications utilizing SSL or TLS must be signed by a well-known and trustworthy authority.

[8] https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexc.pdf

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with this policy may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
Cryptographic[9]	Pertaining to, or concerned with, cryptography.
Cryptography[10]	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorised use, or prevent their undetected modification.
Hash Algorithm[11]	Algorithm that creates a hash based on a message.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

10.0 Related Documents

NIST Federal Information Processing Standard (FIPS) Publication 140-2 [12]

NIST Federal Information Processing Standard (FIPS) Publication 198-1 [13]

NIST Federal Information Processing Standard (FIPS) Publication 180-4 [14]

NIST Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms [15]

[9] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/cryptographic

[10] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/cryptography

[11] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/hash_algorithm

[12] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/publications/detail/fips/140/2/final

[13] *Retrieved from* NIST Information Technology Laboratory Computer Security Resource Center CSRC*:* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

[14] *Retrieved from* NIST Information Technology Laboratory Computer Security Resource Center CSRC*:* https://csrc.nist.gov/publications/detail/fips/180/4/final

[15] *Retrieved from* NIST Information Technology Laboratory Computer Security Resource Center CSRC*:* https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final