Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to establish standards for the use of cryptographic algorithms and technologies within the organization. This policy aims to ensure that only strong, publicly vetted encryption algorithms are employed to protect the confidentiality and integrity of organizational data. It also serves to provide guidance regarding compliance with applicable regulations, particularly concerning the implementation and potential export of encryption technologies.

2.0 Scope

This policy applies to all employees, contractors, vendors, and affiliates of the organization involved in the selection, implementation, or management of systems or processes that utilize encryption for protecting organizational data.

3.0 Policy Statements

The following standards define the acceptable use of encryption algorithms within the organization:

3.1 Approved Encryption Algorithms

* Encryption algorithms used for protecting organizational data must be selected from internationally recognized, publicly reviewed, and currently accepted standards.
* Proprietary or non-standard encryption algorithms are prohibited unless explicitly reviewed, approved, and formally excepted by the designated IT authority (e.g., Precision Computer team) based on a thorough security assessment.

3.2 Symmetric Encryption

* For symmetric encryption (where the same key is used for encryption and decryption), ciphers must meet or exceed the security level defined as "AES-compatible" or "partially AES-compatible" by relevant industry bodies (e.g., IETF/IRTF guidance) or be approved under current U.S. National Institute of Standards and Technology (NIST) standards, such as FIPS 140-2 (or its successors).
* The use of the **Advanced Encryption Standard (AES)** with appropriate key lengths (e.g., 128 bits or higher, preferably 256 bits for new implementations) is the required standard for symmetric encryption unless a specific, approved exception exists.

3.3 Asymmetric Encryption

* For asymmetric encryption (using public/private key pairs), algorithms must meet the standards defined in NIST FIPS 140-2 (or its successors).
* The use of **RSA** (with key lengths of 2048 bits or higher, 3072 bits recommended for new

implementations) or **Elliptic Curve Cryptography (ECC)** (using NIST-approved curves like P-256 or higher) is required for asymmetric encryption. Secure padding schemes (e.g., OAEP for RSA) must be employed.

3.4 Hash Functions

* Cryptographic hash functions used for integrity checks, digital signatures, or other security functions must adhere to current NIST guidance (e.g., the NIST Policy on Hash Functions).
* Algorithms such as SHA-256, SHA-384, SHA-512, or newer SHA-3 family algorithms are required. The use of deprecated algorithms like MD5 or SHA-1 for security purposes is prohibited.

3.5 Digital Signature Algorithms

* Algorithms used for digital signatures must provide an appropriate level of security, corresponding to the requirements for asymmetric encryption and hash functions. Approved algorithms include:
    * **ECDSA** (Elliptic Curve Digital Signature Algorithm) using approved curves (e.g., P-256 or higher). Implementation should consider relevant standards (e.g., RFC6090) to address potential issues.
    * **RSA** (using key lengths specified in section 3.3) with secure padding schemes (e.g., PSS) and appropriate message hashing (as per section 3.4).
    * Other NIST-approved hash-based signature schemes may be considered where appropriate.

3.6 Key Management

* Cryptographic keys must be generated, stored, distributed, rotated, and destroyed securely in accordance with established cryptographic best practices and organizational key management procedures (which may be detailed in a separate Key Management Policy or Standard).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including but not limited to, configuration audits of systems, review of security architecture designs, internal and external security assessments, and analysis of reports from security tools. Feedback will be provided to the policy owner and relevant management.

4.2 Exceptions

Any exception to this policy requires formal, documented justification detailing the business need and compensating controls, and must receive advance approval from the designated IT authority (e.g., Precision Computer team). Approved exceptions will be reviewed periodically.

4.3 Enforcement

Failure to comply with this policy may result in the disabling of non-compliant systems or applications, and may lead to disciplinary action for responsible personnel, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Referenced Standards and Definitions

* **NIST FIPS 140-2 (and successors):** U.S. government standard for cryptographic modules.
* **NIST Policy on Hash Functions:** Guidance on acceptable cryptographic hash algorithms.
* **AES (Advanced Encryption Standard):** The standard symmetric encryption algorithm.
* **RSA (Rivest–Shamir–Adleman):** A widely used public-key (asymmetric) algorithm.
* **ECC (Elliptic Curve Cryptography):** An approach to public-key cryptography based on elliptic curves.
* **ECDSA (Elliptic Curve Digital Signature Algorithm):** A digital signature algorithm using ECC.
* **SHA (Secure Hash Algorithm):** A family of cryptographic hash functions (e.g., SHA-256, SHA-512).
* **Proprietary Encryption:** Encryption algorithms developed privately without public review, generally discouraged due to lack of vetting.

Revision #3
Created 28 August 2024 16:47:39 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery