Cryptography Policy

Policy Owner: Leonard Henriquez

Effective Date: December 22, 2022

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys and cryptographic methods throughout the entire encryption lifecycle.

Scope

All information systems developed and/or controlled by Capsule SAS which store or transmit confidential data.

Policy

Capsule SAS shall evaluate the risks inherent in processing and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57.

Customer or confidential company data must utilize strong ciphers and configurations in accordance with vendor recommendations and industry best practices including NIST when stored or transferred over a public network.

Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

The following table includes the recommended usage for cryptographic keys:

Domain	Key Type	Algorithm	Key Length	Max Expiration
Web Certificate	RSA or ECC with SHA2+ signature	RSA or ECC with SHA2+ signature	2048 bit or greater/RSA, 256bit or greater/ECC	Up to 1 year
Web Cipher (TLS)	Asymmetric Encryption	Ciphers of B or greater grade on SSL Labs Rating	Varies	N/A
Confidential Data at Rest	Symmetric Encryption	AES	256 bit	1 Year
Passwords	One-way Hash	Bcrypt, PBKDF2, or scrypt, Argon2	256 bit+10K Stretch. Include unique cryptographic salt+pepper	N/A
Endpoint Storage (SSD/HDD)	Symmetric Encryption	AES	128 or 256 bit	N/A

Exceptions

Requests for an exception to this policy must be submitted to the Chief Technology Officer (CTO) for approval.

A documented exception is required prior to moving, copying, or storing customer or company confidential data on any media or removable device; all portable devices and removable media containing sensitive data must be encrypted using approved standards and mechanisms.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	22-dec-2022	First Version	Léonard Henriquez	Dan Elkaïm