Aberrant Open-ISM™

ENCRYPTION POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

PROPRIETARY

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

PROPRIETARY

TABLE OF CONTENTS

PROPRIETARY

PROPRIETARY

1 OVERVIEW

Encryption if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise the data. While users may understand it's important to use encryption for electronic communications, they may not be familiar with minimum standards for protection using encryption keys.

2 SCOPE OF PURPOSE

2.1 SCOPE OF POLICY

This policy applies to any encryption methods listed below and to the person responsible for any encryption keys listed below. The encryption keys covered by this policy are:

- encryption keys issued by <<Company Name>>;
- encryption keys used for <<Company Name>> business;
- encryption keys used to protect data owned by <<Company Name>>.

The public keys contained in digital certificates are specifically exempted from this policy. This policy applies to all <<Company Name>> employees and affiliates.

2.2 PURPOSE OF POLICY

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 Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

This policy outlines the requirements for encryption that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

PROPRIETARY

2.3 PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Relevant legislative and regulatory rules regarding the protection and privacy of personally identifiable information (PII) or cardholder data must utilize cryptographic controls described in this policy.

2.4 REGULATION OF CRYPTOGRAPHIC CONTROLS

Cryptographic controls must be deployed and applied in compliance with all applicable laws, regulations or contractual requirements. Cryptographic controls should adhere to applicable standards and industry best practice.

3 POLICIES

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

3.1 PUBLIC KEY ENCRYPTION KEYS

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued.
Public-private key pairs may be generated in software on the end user's computer. Public-private keys should always be stored at rest in an encrypted state that conforms to <<Company Name>>'s encryption standards.

The security personnel shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with <<Company Name>> Password Policy. Security representatives will store and protect the escrowed keys as described in the <<Company Name>> Certificate Practice Statement Policy. The maximum key life provision is one year.

3.2 PUBLIC KEY INFRASTRUCTURE (PKI) KEYS OUTSIDE THE ORGANIZATION

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A

PROPRIETARY

web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

3.3 PGP KEY PAIRS

If the business partner requires the use of PGP, the public-private key pairs should be stored on encrypted disk that conforms to <<Company Name>>'s encryption standard—preferably in <<Company Name>>'s configuration store which is encrypted at rest using AES256.

3.4 PINS, PASSWORDS, AND PASSPHRASES

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in <<Company Name>>'s Password Policy.

3.5 HTTP COOKIES

Only HTTP Cookies that are secure via TLS 1.2 are approved for the storage of information on client machines. Information that is stored in cookies must be encrypted with AES256 or higher.

3.6 HTTP COOKIE AUTHORIZATION TOKENS

Web based authorization tokens require addition security to ensure data integrity and the authentication of a request. <<Company Name>> requires HMACSHA256, or higher, to be used to safeguard tokens used for web based authorization.

3.7 USER SECRETS

User secrets should be stored in encrypted hashes that conform to <<Company Name>>'s encryption policy. Hashed secrets must incorporate a 32-bit salt that is unique for each user.

3.8 LOSS AND THEFT

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to the CTO. Security personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

3.9 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

PROPRIETARY

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.

3.9.1 APPROVED ENCRYPTION ALGORITHMS

Type	Algorithm	Key Length (min)	Additional Comment
Hash Function	**SHA-2**	224+bits	
Symmetric (Secret) Keys	**AES**	256 bits	Minimum of 2 rounds
Asymmetric (Private/Public) Keys	**RSA**	2048 bits	
Asymmetric (Private/Public) Keys	**ECC**	256 bits	

3.9.2 APPROVED CIPHER SUITES

The following list shows Cipher Suites in order of strength with the strongest first. When possible, the most secure suite should be used.

Order	Key Exchange Algorithm	Encryption Algorithm
1	Elliptic Curve Diffie-Hellman (ECDH)	AES in Galois Counter Mode (AESGCM)
2	Diffie-Hellman (DH)	AES in Galois Counter Mode (AESGCM)
3	Elliptic Curve Diffie-Hellman (ECDH)	AES256

3.10 DATA AT REST

3.10.1 WORKSTATION DISK ENCRYPTION

Full disk encryption shall be used on all laptops and high-risk desktops.

3.10.2 PORTABLE MEDIA AND ENCRYPTION

All data on portable media must be encrypted. Only authorized portable media devices and encryption methods shall be used.

3.10.3 STORAGE MEDIA

Encryption at rest is required for storage media that holds customer data or data that is sensitive in nature—e.g. proprietary or confidential data. PII or sensitive information such as passwords should hashed and salted with a unique value for each user.

PROPRIETARY

3.11 DATA IN TRANSIT

Secure data transmission protocols are required to protect credentials and other Confidential Information in accordance with the Data Security & Confidentiality Standard. Data transmission protocols used should be the latest supported version.

Secure Protocols	Minimum Standard	Additional Comment
Transport Layer Security (TLS)	Version 1.2	Version degradation should be disabled for legacy clients.
Internet Protocol Security (IPSEC)	Version 2.0	

3.11.1 WIRELESS NETWORKS

Ensure wireless networks transmitting data use industry best practices to implement strong encryption for authentication and transmission.

3.11.2 IPSEC OVER VPN

VPN users must authenticate via multifactor authentication (username, password, and mobile device alert) prior to being granted remote access. Authorization should be restricted via role-based security privileges defined within the access control system.

3.11.3 OUTBOUND TLS

Outbound TLS should leverage a cloud access security broker (CASB).

3.12 KEY POLICY

In general, <<Company Name>> adheres to the NIST Policy on Hash Functions used for keys.

3.12.1 KEY AGREEMENT AND AUTHENTICATION

- 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 TLS must have the certificates signed by a known, trusted provider.

3.12.2 KEY MANAGEMENT, ROTATION AND STORAGE

PROPRIETARY

- All keys stored on <<Company Name>>'s network is encrypted using the AES-256 algorithm. <<Company Name>> uses a dedicated high availability pair of DSMs that are separated over the WAN.
- Keys held in the DSM are rotated annually.
- Key Owners may delegate to Custodians encryption key administrative and maintenance responsibilities.
- Key Owners and Custodians must formally acknowledge that they understand the requirements and responsibilities of their key custodian role on an annual basis.
- Keys must be distributed, transported and stored in a manner that prevents modification, substitution or disclosure of clear text or contents of encrypted keys before, during, or after the period in which the keys are in service.
- Key custody must have an audit log to maintain accountability.

3.12.3 KEY GENERATION

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Keys must be administered in physically secured internal facilities where access is limited to authorized personnel.
- Keys must be managed with extreme care to prevent compromise of keys and related data.
- A data key or key pair must not be disclosed to a third party unless there is a business need to know.
- When feasible, two custodians shall be involved with the creation, distribution and management of encryption keys.
- Keys taken out of service shall not be reused.

3.12.4 MANAGEMENT OF COMPROMISED KEYS

- Compromised keys are invalidated and archived in a secure manner. Once the method of how they were compromised is determined they are re-generated in-line with Key Generation guidelines.

3.13 POLICY COMPLIANCE

3.13.1 COMPLIANCE MANAGEMENT

The CISO or delegated security personnel will verify compliance to this policy through various methods, including but not limited to, walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

PROPRIETARY

3.13.2 EXCEPTIONS

Any exception to the policy must be approved by the CISO in advance.

3.13.3 NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

PROPRIETARY

4 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

5 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

PROPRIETARY

6 LICENSE INFORMATION

This work is licensed under a Creative Commons Attribution-NonCommercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode)

To further clarify the Creative Commons license related to the Open-ISM™ content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to Aberrant, Inc., and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the Open-ISM, you may not distribute the modified materials. Users of the Open-ISM framework are also required to refer to (http://www.aberrant.io/open-ism/license) when referring to the Open-ISM to ensure that users are employing the most up-to-date guidance. Commercial use of the Open-ISM is subject to the prior approval of Aberrant, Inc.