Cryptography Policy

v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information **2**

1 Introduction **4**

2 Policy on the use of Cryptographic Controls **4**

2.1 Risk Assessment 4

2.1.1 Technique Selection 5

2.2 Deployment 5

2.3 Testing and Review 5

3 Key management **6**

1 Introduction

A key component in the set of controls available to organizations to protect their classified information is the use of cryptographic techniques to “scramble” data so that it cannot be accessed without knowledge of a key.

Cryptographic controls can be used to achieve several information security-related objectives, including:

- Confidentiality – ensuring that information cannot be read by unauthorised persons
- Integrity – proving that data has not been altered in transit or whilst stored
- Authentication – proving the identity of an entity requesting access to resources
- Non-repudiation – proving that an event did or did not occur or that a message was sent by an individual

The need for cryptographic controls will be highlighted from the Jadarah For Dept Collections Co. risk assessment and will obviously not be applicable in all cases. However, where their use can provide the required level of protection, they must be applied according to the provisions set out in this policy.

This control applies to all systems, people and processes that constitute the organization’s information systems, including board members, directors, employees, suppliers and other third parties who have access to Jadarah For Dept Collections Co. systems.

2 Policy on the use of Cryptographic Controls

In order to identify those areas in which the deployment of cryptographic techniques will be useful, Jadarah For Dept Collections Co. will take a managed approach as follows.

2.1 Risk Assessment

The first step will be to undertake a risk assessment in line with the ISO/IEC 27001 Information Security standard. For each of the information assets identified within the organization, possible threats will be assessed together with their likelihood and impact should they occur.

The following documents within the Jadarah For Dept Collections Co. Information Security Management System set out how this is achieved:

- Risk Assessment and Treatment Process
- Risk Assessment Report
- Risk Treatment Plan

Requirements for the use of cryptographic techniques will be identified in the last of these documents. This risk treatment plan will show in overview where cryptographic techniques must be applied and in what form to achieve the level of protection needed.

In general terms, the use of cryptography will tend to be applicable in the protection of information classified within the organization as “Restricted” or “Confidential” (see Information Classification Procedure).

In addition, cryptography should be seriously considered in the following scenarios:

- On mobile devices such as laptops, tablets and smartphones
- For authorised use of removable media such as USB memory sticks

- Where classified data is transmitted across communications lines that extend beyond the boundaries of the organization e.g., over the Internet
- Where cloud services are used, regardless of the type of cloud service (e.g., IaaS, PaaS, SaaS)

2.1.1 Technique Selection

Once the general need for the use of cryptography has been identified by the risk assessment, a decision needs to be made about which specific techniques will be deployed. This will also involve the selection and possible purchase of software or hardware in order to implement the technique.

Note that the selection of such techniques must take into account any current regulations or national restrictions on the procurement and use of cryptographic technology.

These may affect the type, strength and quality of the encryption algorithm used.

In general, the policy of Jadarah For Dept Collections Co. is to use the following techniques for the relevant business process or situation:

PROCESS/SITUATION	TECHNIQUE	SPECIFIC GUIDANCE
Storage of data in the cloud	AES-256 encryption at rest	Keys not to be held by the CSP
E-Commerce transactions over the Internet	Symmetric encryption using TLS (Asymmetric techniques used to share session key)	RSA to be used for public key cryptography. Certificates to be obtained from a reputable supplier
Protection of data on removable media	Symmetric encryption	AES-256 encryption to be used where available
Protection of passwords on systems	All passwords must be hashed	MD5 hashing to be used where available
Email Security	Symmetric/asymmetric encryption using S/MIME	Features available in the relevant email client should be used to simplify the process
Remote Access	Virtual Private Network (VPN) using TLS	An IPSec VPN may be used where permitted by the *Network Security Policy*

The continued use of the specified techniques will be evaluated on each review of this policy.

2.2 Deployment

The deployment of cryptographic techniques must be managed carefully to ensure that the desired level of security is in fact achieved. Where possible, more than one member of staff will be closely involved in the deployment in order to avoid both a single point of failure for support and to allow segregation of duties to take place.

Close consideration must be given to the on-going operation of the installed encryption so that documented operational procedures are fully in place and the relevant staff are trained in them.

2.3 Testing and Review

Once deployed, it is critical that the security of the encryption be tested under as realistic conditions as possible in order to identify any weaknesses. Such testing must cover the use of:

- Commonly-available software tools to try to break the encryption
- Social engineering methods to try to discover the key
- Interception of encrypted data at various points in its transmission

The results of tests will be formally reviewed, and lessons learned will be applied to the tested situation and communicated to other areas in which encryption is used in the organization.

3 Key management

It is vital that cryptographic keys are protected from modification, loss, destruction and unauthorised disclosure. A lifecycle approach will be taken to key management which will require the creation of specific procedures to cover the following stages:

- Key generation
- Distribution of keys to point of use
- Storage at point of use
- Backup as protection against loss
- Recovery in the event of loss
- Updating keys once expired
- Revoking if compromised
- Archiving once expired
- Destroying when no longer required
- Logging and auditing of key management related activities

These procedures will take account of the specific circumstances in which encryption will be used.

In principle, private asymmetric keys and symmetric keys shall only exist in the following secure forms:

1. As cleartext within the memory of a hardware-based encryption device
2. As ciphertext outside the memory of a hardware-based encryption device
3. As two or more key fragments either in cleartext or ciphertext, managed using dual control with split knowledge

Use of one of these three forms will ensure that the confidentiality of private asymmetric and symmetric keys is always maintained. Public asymmetric keys are generally available and so do not require protection. Their integrity and authenticity do however need to be protected and this must be achieved via the use of a signature from a reputable certification authority.

Where key management functionality is provided as part of a cloud service, the following information must be requested about the facilities provided by the CSP:

- Type of keys
- Key management system specifications
- Recommended key management procedures for each stage of the key management lifecycle as defined above

In the event that cryptographic keys are subject to a request by a government agency, Jadarah For Dept Collections Co. will comply with all legally authorised requests in a timely manner. The compliance process will be subject to senior management oversight and control.