ENCRYPTION & KEY MANAGEMENT POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Application of Encryption 4

2.2 Robust Solutions 4

2.3 Public Algorithms 4

2.4 Key Management Procedures 4

2.5 Key Compromise and Revocation 4

2.6 Key Custodians 4

2.7 Secure Transmission on Public / Untrusted Networks 4

2.8 Split Knowledge / Dual Control 4

2.9 Compliance with Local Regulation 5

3. Policy Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Exception Process / Glossary 7

4.1 Exception Process 7

4.2 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Document Distribution 8

6. Appendix A - Encryption Key Custodian Form 9

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The objective of this policy is to provide information security requirements for the implementation and use of encryption within XXXX (XXXX) systems. This policy also aims to provide guidance on the management of associated encryption keys as well as some high-level consideration points for selecting the appropriate cryptosystem.

The scope of this policy includes all applications and systems utilising encryption.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-005- Data Handling &Retention Policy*
* *XXXX-STD-ALL-018- Encryption & Key Management Standard(s)*

# Policy Statements

## Application of Encryption

The application of Encryption must be based on an assessment of the sensitivity level of the information to be stored or transmitted and the security controls over the storage or transmission environment. *XXXX-POL-ALL-005- Data Handling & Retention Policy* refers.

## Robust Solutions

Encryption solutions must be robust and kept in line with recognised standards, taking into account changes in technology and advances in encryption.

## Public Algorithms

The use of encryption must be limited to algorithms that have received public review and have been proven to work effectively.

## Key Management Procedures

For every encryption implementation, well documented and industry accepted key management procedures are required.

## Key Compromise and Revocation

Encryption keys that have been compromised or are suspected of being compromised must be revoked immediately. Encryption keys must not be used when revoked or when no longer valid.

## Key Custodians

Access to encryption key must be restricted to the fewest number of key custodians necessary to provide both operational function, and appropriate incident response and disaster recovery support.

Key custodians must acknowledge that they understand and accept their key-custodian responsibilities.

See Appendix A for Key Custodian Request Form.

## Secure Transmission on Public / Untrusted Networks

Protocols used in the security of data transmission over untrusted networks must comply with the following:

* Only trusted keys and/or certificates can be accepted;
* Only secure configuration are supported, and;
* The proper encryption strength is use for the encryption methodology in use.

## Split Knowledge / Dual Control

If manual clear-text encryption key-management operations are used, these operations must be managed using split knowledge and dual control.

## Compliance with Local Regulation

Cryptosystems utilised must comply with local laws governing encryption use, import, and export where applicable.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For a selection of encryption implementations, evidence that documented and approved key management procedures exist. | * Copies of the documented key management procedures including approvals |
| For a selection of client server communication, evidence that an appropriate Transport layer security is been used | * Confirm the version of TLS been use and it has not expired |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| Hash / Hash Function | An algorithm that turns a variable-sized amount of text into a fixed-sized output (hash value). |
| Key | A numeric code or character string that is used to encrypt text for security purposes. |
| Key Management | The creation, distribution and maintenance of a secret key. |
| Proprietary Algorithm | An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government. |
| Symmetric or Static Key | A single key is used for both encryption and decryption of the data. The key must be shared between both ends of the encrypted transmission (examples include RC5, 3DES, and AES). |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* IT
* Information Security

# Appendix A - Encryption Key Custodian Form

**XXXX Encryption Key Custodian Form**

Encryption key custodians are those person(s) delegated the responsibility of managing, handling and protecting access to XXXX encryption keys. Custodians are responsible for the confidentiality and integrity of key components in their custody. In particular, the custodian has responsibility to:

* Implement all encryption key controls as specified and documented in information security policies and procedures.
* Provide safeguards for encryption keys during generation, loading and storage.
* Administer access to the encryption keys and make provisions for timely detection, reporting, and analysis of unauthorised attempts to gain access to these keys.
* Control access and secrecy of the combination of the safe containing the clear-text encryption keys.
* Complete the encryption Key Management Log for any activity involving encryption keys.
* Participation in the encryption key generation, distribution, change, and destruction processes.

By signing this form I acknowledge that I understand and accept of my responsibilities as key custodian.

Key Custodian Signature Date

Printed Name