Encryption & Key Management Standard

*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 Industry Configuration Standards 3

1.5 Related Documents / References 3

2. Standard Statements 4

2.1 Encryption & Key Management Standards 4

3. Standard 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 Distribution 8

# Introduction

## Document Definition

This document is a Standard.

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

## Objective

The protection of electronic information and access to information systems is vitally important - especially with the ever increasing and greater demand. Encryption & Key Management provides an enhanced level of security from unauthorized access, disclosure or use when information is being transmitted or kept in storage. It includes protection of sensitive information and communications, key management, and procedures to ensure encrypted information can be recovered by the bank if necessary.

## Scope

### Applicability to employees

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

### Applicability to External Parties

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

### Applicability to Assets

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

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/
* Security Technical Implementation Guides (STIGs): http://iase.disa.mil/stigs

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## Encryption & Key Management Standards

1. All cryptographic keys shall be protected against modification, loss, and destruction. In addition, secret and private keys shall be protected against unauthorized disclosure.
2. Equipment used to generate, store and archive keys shall be physically protected from unauthorized access.
3. The key management system shall be based on an agreed set of procedures, and secure methods for:
4. Generating keys for different cryptographic systems and different applications.
5. Generating and obtaining public key certificates.
6. Distributing keys to intended users, including how keys shall be activated when received.
7. Storing keys, including how authorized users obtain access to keys.
8. Changing or updating keys including rules on when keys shall be changed and how this will be done.
9. Dealing with compromised keys.
10. Revoking keys including how keys shall be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves the Bank (in which case keys must also be archived).
11. Recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information.
12. Archiving keys, e.g. for information archived or backed up.
13. Destroying keys.
14. Logging and auditing of key management related activities.
15. In order to reduce the likelihood of compromise, activation, and deactivation dates for keys shall be defined so that the keys can only be used for a limited period. This period shall be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.
16. In addition to securely managing secret and private keys, the authenticity of public keys shall also be considered. This authentication process shall be done using public key certificates which are normally issued by a certification authority, which shall be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.
17. The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, shall cover issues of liability, reliability of services and response times for the provision of services.
18. Encryption keys are a most sensitive type of information, and access to such keys must be strictly limited to those who have a need-to-know, encryption keys must not be revealed to consultants, contractors, or other third parties.
19. The bank’s encryption systems must be designed such that no single person has full knowledge of any single encryption key. This must be achieved by separation of duties and dual control/split custody. Separation of duties refers to use of more than one individual to handle the different steps involved in a certain important activity, while dual control/split custody means that two people must be simultaneously present for an important activity to be accomplished.
20. Key management responsibility may only be delegated to a party who is a confirmed professional staff, does not have any operational audit issue(s) pending against him and has signed a confidentiality agreement.
21. All general-purpose encryption processes running on the bank’s information systems must include key escrow functions. These special functions allow the bank to recover encrypted information in the event of system errors, human errors, or other problems.
22. Encryption keys which have been compromised or revealed to third parties under a key escrow arrangement, must immediately be revoked retroactively to the last known time when the keys were safe.
23. If encryption is used to protect sensitive data resident on computer storage media, the encryption keys and related encryption keying materials (initialization vectors, time-and-date stamps, salt parameters, etc.) used in the encryption process must not be stored anywhere on the storage media in unencrypted form.
24. Whenever encryption is used for data at rest, the sole readable version of data may be deleted only after it is confirmed that the decryption process is able to restore a readable version of the data.

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. 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** |
| Review the bank’s environment where encryption has been implemented. | * Confirm if the encryption standard was followed |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards 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 Standard 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

|  |  |
| --- | --- |
| CA | Certification Authority |
|  |  |

# Document Management

## Document Revision Log

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

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

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

## Distribution

* *Information Security*
* *IT Department*