ENCRYPTION

ewards you for being you
It's a more rewarding way to bank
Barclays Blue Rewards
RSA SecurID

Table of Contents

Version Control

Document Reference: Il7 Security Encryption Policy

Version	Description of change	Date	Author	Approver
0.1				

1. Introduction

An ever-increasing threat environment requires any organization to implement appropriate measures to protect it from information security related threats and to prevent unauthorized data loss or exposure of its information assets to in appropriate disclosure. Il7 Group has updated its policy status to align itself with ISO/IEC 27001:2013 in line with the approved Information Security Management System (ISMS), October 2018.

2. Purpose

The purpose of the Information Security Encryption Policy is to ensure there are mechanisms within each Operating Company as well as Il7 Group to:

- Properly take into account and formulate a cryptographic policy.
- Develop procedure on key management to protect the integrity of cryptographic keys.

3. Audience and Scope

This policy presents the outcomes that must be delivered through standards and procedures implemented by all Il7 Operating Companies including Head Office for Information and Data Encryption Management

It is applicable and binding to all Il7 and Operating Companies employees, including Executive Management, permanent staff, contract and temporary employees.

The audience for this policy is Il7 and the Operating Companies.

4. Review

This encryption policy shall be established, documented and reviewed based on business and information security requirements. It is to be reviewed annually and updated accordingly.

5. Cryptographic Controls

Reference ISO 27001 A.10.1

Policy on the use of cryptographic controls

Reference ISO 27001 A.10.1.1

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

When developing a cryptographic policy, the following should be considered:

- the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected.
- based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required.
- the use of encryption for protection of information transported by mobile or removable media devices or across communication lines.
- the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys.
- roles and responsibilities, e.g. who is responsible for:
    - the implementation of the policy.
    - the key management, including key generation (see 10.1.2).
- the standards to be adopted for effective implementation throughout the organization (which solution is used for which business processes).
- the impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection).

When implementing the organization’s cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see ISO 27001 18.1.5).

Cryptographic controls can be used to achieve different information security objectives, e.g.:

- confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted.
- integrity/authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information.
- non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action.
- authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

Making a decision as to whether a cryptographic solution is appropriate and should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes. A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use. Specialist advice should be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

Key management

Reference ISO 27001 A.10.1.2

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

Cryptographic algorithms, key lengths and usage practices should be selected according to best practice.

Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

- generating keys for different cryptographic systems and different applications.
- issuing and obtaining public key certificates.
- distributing keys to intended entities, including how keys should be activated when received.
- storing keys, including how authorized users obtain access to keys.
- changing or updating keys including rules on when keys should be changed and how this will be done.
- dealing with compromised keys.
- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived).
- recovering keys that are lost or corrupted.
- backing up or archiving keys.
- destroying keys.
- logging and auditing of key management related activities.

To reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period of time defined in the associated key management policy. In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see ISO 27001 15.2).

The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770[2][3][4] provides further information on key management. Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case.