[organization logo]

[organization name]

**POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454540203)

[2. Reference documents 3](#_Toc454540204)

[3. Use of cryptography 3](#_Toc454540205)

[3.1. Cryptographic controls 3](#_Toc454540206)

[3.2. Cryptographic keys 3](#_Toc454540207)

[3.3. Cryptographic information to cloud service customers 4](#_Toc454540208)

[4. Managing records kept on the basis of this document 4](#_Toc454540209)

[5. Validity and document management 5](#_Toc454540210)

# Purpose, scope and users

The purpose of this document is to define rules for the use of cryptographic controls, as well as the rules for the use of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all systems and information used within the ISMS scope.

Users of this document are [job title].

# Reference documents

* ISO/IEC 27001 standard, clauses A.10.1.1, A.10.1.2, A.18.1.5
* ISO/IEC 27017 standard, clauses 10.1.1 and 18.1.5
* ISO/IEC 27018 standard, clauses A.9.2 and A.11.1
* Information Security Policy
* [Information Classification Policy]
* [List of Legal, Regulatory, Contractual and Other Requirements]

# Use of cryptography

## Cryptographic controls

According to the Information Classification Policy, as well as legal and contractual obligations, the organization must protect individual systems or information by means of the following cryptographic controls:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Name of system / type of information*** | ***Cryptographic tool*** | ***Encryption algorithm*** | ***Key size*** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[job title] is responsible for preparing detailed instructions on the use of the mentioned cryptographic tools. Owners of individual assets to which cryptographic controls are applied are responsible for appropriate application of individual cryptographic controls.

## Cryptographic keys

[job title] is responsible for prescribing the following rules regarding key management:

* generating private and public cryptographic keys
* activation and distribution of cryptographic keys
* defining the time limit for the use of keys and their regular updating (in accordance with risk assessment)
* archiving inactive keys which are necessary for encrypted electronic archives
* destruction of keys

Keys are managed by their owners in line with the abovementioned rules.

Cryptographic keys will be protected [provide a description of how keys will be protected against loss, change or destruction]. In the case of loss, corruption or destruction, keys will be recovered [describe method of recovery].

## Cryptographic information to cloud service customers

[job title] is responsible to provide to the cloud service customers information regarding:

* the cryptographic tools used to protect their information
* any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions
* the identity of the countries where the cryptographic tools are used to store or transfer cloud service customers’ data

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Key management records] | [job title]'s computer | [job title responsible for key management] | Only [job title] has access rights to such records | Records are stored for a period of 10 years |
| [Detailed instructions on the use of the cryptographic tools] | [company intranet] | [job title] | Only [job title] has the right to edit and publish the instructions | Instructions that are no longer valid are stored for a period of 5 years |
| [Rules for key management] | [company intranet] | [job title] | Only [job title] has the right to edit and publish the rules | Rules that are no longer valid are stored for a period of 5 years |

Only [job title] can grant other employees access to the any of the abovementioned records.

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once every six months.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

* number of incidents related to loss, compromise or destruction of cryptographic keys
* number of systems to which cryptographic controls are applied contrary to this Policy

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]