[Organization logo]

[Organization name]

POLICY ON THE USE OF ENCRYPTION

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

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [270012]: To learn more about this issue, read this article:

How to use the cryptography according to ISO 27001 control A.10
https://advisera.com/27001academy/blog/2015/12/14/how-to-use-the-cryptography-according-to-iso-27001-control-a-10/

Commented [270013]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. 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 [list the job titles of people who need to comply with this policy].

Commented [270014]: E.g.: top management, IT staff, remote users, etc.

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.31, and A.8.24
- Information Security Policy
- [Information Classification Policy]
- [List of Legal, Regulatory, Contractual and Other Requirements]

Commented [27A5]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

Commented [270016]: If you don't have this List, then list all the legislation and contracts related to the use of cryptography.

3. Use of cryptography

3.1. Cryptographic controls

According to the Information Classification Policy, as well as legal and contractual obligations, the

[redacted]	*Cryptographic tool*	[redacted]	*Key size*
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Commented [270017]: [redacted]

Commented [270018]: List everything that is regulated by the [redacted]

[redacted] responsible for appropriate application of individual cryptographic controls.

Commented [270019]: [redacted]

3.2. Cryptographic keys

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

Commented [2700110]: [redacted]

- [redacted]
- [redacted]
- defining the time limit for the use of keys and their regular updating (in accordance with risk [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

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

[redacted]

Commented [2700111]: [redacted]

Commented [2700112]: E.g.: by means of backup copy

4. 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 3 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 3 years

Commented [2700113]: Alter these records to match the records you already have in your company. If you do not have similar records, you can create new ones in the format that suits you best.

Commented [2700114]: Adjust appropriately.

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

5. 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.

Commented [2700115]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]
- [illegible]

[job title]
[name]

_____
[signature]

Commented [2700116]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.