[organization logo]

[organization name]

**PROCEDURE FOR IDENTIFICATION OF REQUIREMENTS**

|  |  |
| --- | --- |
| 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 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415648115)

[2. Reference documents 3](#_Toc415648116)

[3. Identification of requirements and interested parties 3](#_Toc415648117)

[4. Reviewing and evaluation 3](#_Toc415648118)

[5. Managing records kept on the basis of this document 4](#_Toc415648119)

[6. Validity and document management 4](#_Toc415648120)

[7. Appendices 4](#_Toc415648121)

# Purpose, scope and users

The purpose of this document is to define the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements related to information security and business continuity, and responsibilities for their fulfillment.

This document is applied to the entire Information Security Management System (ISMS).

Users of this document are all employees of [organization name].

# Reference documents

* ISO/IEC 27001 standard, clause 4.2; control A.18.1.1
* ISO 22301 standard, clause 4.2
* Information Security Management System Policy
* Business Continuity Policy

# Identification of requirements and interested parties

[job title] is responsible for identifying (1) all persons or organizations that can affect or can be affected by information security or business continuity management (interested parties), and (2) all related legal, regulatory, contractual and other requirements.

[job title] will define who will be responsible for compliance with each individual requirement, and which interested parties are to be notified when changes occur.

[job title] must list all requirements, interested parties, and responsible persons in “List of legal, regulatory, contractual and other requirements,” and publish that List in .

Every employee in [organization name] must notify [job title] if he/she comes across any new legal, regulatory, contractual or other requirement that might be relevant to information security and business continuity management.

# Reviewing and evaluation

[job title] is responsible for reviewing the List of legal, regulatory, contractual and other requirements at least every 6 months, and for updating it as necessary. [job title] will notify all relevant interested parties upon each update.

[job title] is responsible for evaluating the compliance of ISMS with relevant legal, regulatory and contractual requirements at least once a year.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
| List of legal, regulatory, contractual and other requirements (in electronic form) | Organization's intranet | [job title] | Only [job title] is authorized to edit data | Old versions of the List are archived for 3 years |

# 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 a year.

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

* number of organization's obligations that existed, but were not identified
* number or amount of penalties paid, resulting from lack of compliance with obligations
* number of days that the compliance with obligations was late

# Appendices

* Appendix: List of Legal, Regulatory, Contractual and Other Requirements

[job title]

[name]

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

[signature]