[Organization logo]

[Organization name]

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

PROCEDURE FOR IDENTIFICATION OF REQUIREMENTS

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

Commented [270012]: 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 3
2. REFERENCE DOCUMENTS 3
3. IDENTIFICATION OF REQUIREMENTS AND INTERESTED PARTIES 3
4. REVIEWING AND EVALUATION 3
5. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4
6. VALIDITY AND DOCUMENT MANAGEMENT 4
7. APPENDICES 4

1. 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].

2. Reference documents

- ISO/IEC 27001 standard, clause 4.2, and A.5.31
- ISO 22301 standard, clause 4.2
- Information Security Policy
- Business Continuity Policy

3. Identification of requirements and interested parties

[redacted] related legal, regulatory, contractual and other requirements.

[redacted] Regulatory, Contractual and Other Requirements," and publish that List in [location].

Every employee in [organization name] must notify [job title] if he/she comes across any new legal, [redacted]

4. Reviewing and evaluation

[Job title] is responsible for reviewing the List of legal, Regulatory, Contractual and Other [redacted] contractual requirements at least once a year.

Commented [270013]: Delete this if only business continuity is implemented.

Commented [270014]: Delete this if business continuity is not implemented.

Commented [270015]: Or write "Business Continuity Management System (BCMS)" if you are implementing business continuity only.

Commented [270016]: Include the name of your company.

Commented [270017]: Remove this if business continuity is not implemented.

Commented [27A8]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "05_General_Policies".

Commented [270019]: Remove this if business continuity is not implemented.

Commented [2700110]: This article will help you to identify requirements:

How to identify ISMS requirements of interested parties in ISO 27001 https://advisera.com/27001academy/blog/2017/02/06/how-to-identify-isms-requirements-of-interested-parties-in-iso-27001/

Commented [2700111]: This article will help you to identify the interested parties:

Who are interested parties, and how can you identify them according to ISO 27001 and ISO 22301? https://advisera.com/27001academy/knowledgebase/how-to-identify-interested-parties-according-to-iso-27001-and-iso-22301/

Commented [2700112]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager etc.

Commented [2700113]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Process Owner, Business Area Responsible, etc.

Commented [2700114]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, etc.

Commented [2700115]: [redacted]

Commented [2700116]: Include the name of your company.

Commented [2700117]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Compliance Officer, etc.

Commented [2700118]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Process Owner, Business Area Responsible, etc.

Commented [2700119]: Change this as necessary.

Commented [2700120]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Process Owner, Business Area Responsible, etc.

Commented [2700121]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Process Owner, Business Area Responsible, etc.

Commented [2700122]: Or "BCMS"

Commented [2700123]: To simplify the procedure, this can be done by internal auditor.

Commented [2700124]: Change this as necessary.

5. 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

Commented [2700125]: Adapt the period in this column to your specific needs.

Commented [2700127]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, Process Owner, Compliance Officer, etc.

Commented [2700128]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, Process Owner, Compliance Officer, etc.

Commented [2700126]: Change as appropriate.

6. 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.

Commented [2700129]: E.g.: Business Continuity Manager, Information Security Manager, Security Manager, Process Owner, Compliance Officer, etc.

[redacted]
considered:

- [redacted]
- [redacted]
- [redacted]

7. Appendices

- [redacted]

[job title]
[name]

_____
[signature]

Commented [2700130]: Only necessary if the Procedure for Document Control prescribes that paper documents must be signed.