Seventh loop Tech

PROCEDURE FOR IDENTIFICATION OF REQUIREMENTS

Code:	005
Version:	0.1
Date of version:	2025/08/21
Created by:	Hammad Zahid Ali
Approved by:	Taimor Ijlal, CISO
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
2025-08-21	0.1	Abdullah	Basic document outline

Table of contents

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 Seventh Loop Tech.

2. Reference documents

- ISO/IEC 27001 standard, clause 4.2; control A.18.1.1
- ISO 22301 standard, clause 4.2
- ISO/IEC 27017 standard, clause 18.1.1
- ISO/IEC 27018 standard, clauses A.9.2 and A.11.1
- Information Security Management System Policy
- Business Continuity Policy

3. Identification of requirements and interested parties

CISO 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), (2) all geographical locations from where the Seventhloop provides cloud services, especially those acting as Personally Identifiable Information (PII) processors, and (3) all related legal, regulatory, contractual and other requirements.

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

CISO/Compliance Officer must list all requirements, interested parties, geographical locations, and responsible persons in “List of legal, regulatory, contractual and other requirements,” and publish that List in .

Every employee in Seventh Loop Tech must notify CISO/Information Security Manager if he/she comes across any new legal, regulatory, contractual or other requirement that might be relevant to information security and business continuity management.

4. Reviewing and evaluation

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

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

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 Z:\\Sharedrive\ISMS	CISO	Only CISO is authorized to edit data	Old versions of the List are archived for 3 years

6. Validity and document management

This document is valid as of 2026/08/29.

The owner of this document is CISO, 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

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

7. Appendices

- Appendix: Form – List of legal, regulatory, contractual and other requirements

Chief Information Security Officer (CISO)
Taimor Ijlal

_____

[signature]