(Organization logo and name and date of creation of the template)

**Requirements Identification Procedure**

|  |  |
| --- | --- |
| Document ID |  |
| Version |  |
| Version created date |  |
| Creator |  |
| Approved By |  |
| Level of Confidentiality |  |

**Modify History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modified By | Explanation of the modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Usable party(s), Objective and the focus area 5](#_Toc84476445)

[2. Reference documents 5](#_Toc84476446)

[3. Requirements and interested parties Identification 5](#_Toc84476447)

[4. Evaluation, Monitoring and reviewing 6](#_Toc84476448)

[4.1. Evaluation & Monitoring 6](#_Toc84476449)

[4.2. Management reviewing 7](#_Toc84476450)

[4.2.1. Management review details 7](#_Toc84476451)

[5. Maintaining control of records based on this document 8](#_Toc84476452)

[6. Validity and Document Management 8](#_Toc84476453)

# Usable party(s), Objective and the focus area

Objective

The purpose of this material is to clarify the process for identifying interested and legal organizations, as well as the responsibility for upholding regulatory, a contract, and other information security requirements.

Focus Area

This document is applicable to the whole ISMS system.

Usable parties

All [organization name] workers may use this document.

# Reference documents

* ISO/IEC 27001 standards clause 4.2.
* ISMS Policy.

# Requirements and interested parties Identification

The [job title] is in charge of defining (1) all people or organizations who can impact or be affected by information security management [interested parties], as well as (2) all legal, regulatory, contractual, and other needs.

The [job title] will determine who is accountable for ensuring that each criterion is met, as well as who should be alerted when any modifications occur.

[Job title] must produce a "List of legal, regulatory, contractual, and other requirements" that includes all needs, interested parties, and accountable individuals, and publish that list in the Organization.

# Evaluation, Monitoring and reviewing

## Evaluation & Monitoring

What has to be watched, assessed, and evaluated inside the organisation should be decided upon before conducting the evaluation.

These are the main activities must be monitored for implement security in the organization.

* What tasks and procedures are the most frequently subject to occur serious threats?
* What activities have the greatest severe vulnerabilities built-in?
* What can be monitored and used to create useful and timely information?
* For each monitoring process the organization should define these details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Monitoring process ID | Date | Responsible person | Result reporting way and the purpose of getting results | Are any unacceptable performance detected during the process | What are the solution if any errors occurred |
| Ex; 001 | 02/07/2021 | Monitoring Manager | Way – through electronic media purpose - To ensure the system security is update | - | - |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Management reviewing

To ensure that the organization's information security management system remains adequate, sufficient, and effective, top management is in charge of performing recurring evaluations.

### Management review details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Review no. | Date | Responsible party who did the review | Status of action from previous reviews | Change in internal and external issues | Feedback about the performance | Results of risk assessments and risk treatment plans | Opportunities for imporvements |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Maintaining control of records based on this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of the record | Storage Location | Responsible person for storage | Controls for record protection | Retention time |
|  |  |  |  |  |

# Validity and Document Management

The document is valid as of [date]

The owner of this document, [job title], oversees checking and, if necessary, updating the record at least once a year.

When implementing the procedure the following criteria must be considered

* All activities must be monitored and evaluated effectively and securely
* All monitoring processes details must be included to the monitoring process details table.

[job title]

[name]

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

[signature]