**Procedure Identification**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Number: |  |
| 2. | Version History: |  |
| 3. | Created Date: |  |
| 4. | Created By: |  |
| 5. | Approved By: |  |
| 6. | Contact: |  |

Document Modify History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modified By | Modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Objectives, Focus area and Usable parties 4](#_Toc179656724)

[Reference Documents 4](#_Toc179656725)

[Requirements and interested parties’ Identification 5](#_Toc179656726)

[Evaluation, Monitoring and reviewing 6](#_Toc179656727)

[List of Legal and Contractual Requirements Register 8](#_Toc179656728)

[Maintaining Control of records based on this document 9](#_Toc179656729)

[Validity and Document Management 9](#_Toc179656730)

# Objectives, Focus area and Usable parties

**Objectives:**

This documentation's goal is to provide an overview of the steps involved in locating pertinent parties, laws, contracts, regulations, and other information security duties, as well as the tasks involved in completing them.

**Focus Area:**

This document is applicable to the entire scope of the ISMS system.

**Usable Parties:**

This document is applicable to all employees of [organization name].

# Reference Documents

* ISO 27001 Standards
* ISMS policy

# Requirements and interested parties’ Identification

There are two key jobs for the [job title]. It begins by covering the duty to identify all parties that information security management may affect or have an influence on, as well as all responsibilities related to contracts, laws, regulations, and other matters.

The [job title] is responsible for determining who is in charge of ensuring that each requirement is followed and who has to be notified of any changes. Furthermore, [job title] is responsible for compiling an exhaustive "List of legal, regulatory, contractual, and other requirements" that identifies all responsibilities, interested parties who have expressed interest, and persons who must be held accountable, and ensuring that this list is accessible across the organization.

# Evaluation, Monitoring and reviewing

1. **Evaluation and Monitoring**

During the evaluation process, decisions should be made about what needs to be observed, measured, and evaluated inside the organization.

The following actions must be kept an eye on in order to implement security within the organization:

* Identify tasks and procedures that are likely to pose serious threats.
* Identify activities that have serious vulnerabilities.
* Identify elements that are appropriate for tracking in order to produce useful and prompt information.
* For every monitoring process, outline the required details.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Monitoring process ID | Date | Responsible person | Reporting Method and the Purpose of Obtaining Results. | Have any instances of unacceptable performance been identified during the process? | solutions |
| Example :001 | 30/09/2023 | Monitoring Manager | Method - leveraging online channels Objective - To maintain up-to-date system security. | - | - |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Management Reviewing**

The senior management is responsible for regularly reviewing the company's information security management system to ensure it remains relevant, adequate, and effective.

* **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 | Outcomes of Risk Assessments and Plans for Risk Treatment. | Opportunities for improvements |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# List of Legal and Contractual Requirements Register

1. **Applicable Standards:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Standard | Requirements | Applicability | Required: Yes/No | Last Assessed | Next Assessment |
| ISO 27001 | International Information Security Management System | ISO 27001 is the basis and framework for the Information Security Management System (ISMS). |  |  |  |
| NIST | NIST Cyber Security Framework | The Framework provides optional guidance that builds on current standards, guidelines, and practices to help organizations improve their management and reduction of cybersecurity risk. |  |  |  |

1. **Regulatory Requirements:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Regulatory | Requirements | Applicability | Required: Yes/No | Last Assessed | Next Assessment |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Contractual Requirements:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Regulatory | Requirements | Applicability | Required: Yes/No | Last Assessed | Next Assessment |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Legal Requirements:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Legislation | Requirements | Applicability | Required: Yes/No | Last Assessed | Next Assessment |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 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's validity commences on: [date]

With a minimum frequency of once a year, [job title] is the owner of this document and is responsible for periodic checks and necessary updates.

When executing this procedure, the following criteria must be adhered to:

* The guidelines provided in this page must be followed while creating any document.
* Each document must go through a regulated procedure in order to be created, approved, distributed, used, and updated.

[Job Title]

[Name]

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

[Signature]