**General Policies and Procedures**

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](#_Toc179668677)

[Reference Documents 4](#_Toc179668678)

[Terminology used in information Security 5](#_Toc179668679)

[I. Principle 5](#_Toc179668680)

[II. Commitment from the top executives 5](#_Toc179668681)

[III. Objectives of Information Security Policy 5](#_Toc179668682)

[IV. Framework of Information Security Policy 6](#_Toc179668683)

[Information Security Roles and Responsibilities 7](#_Toc179668684)

[Policy Compliance 7](#_Toc179668685)

[Maintaining control of records based on this document 8](#_Toc179668686)

[Validity and Document Management 8](#_Toc179668687)

# Objectives, Focus Area and Usable Parties

**Objectives:**

This top-level Policy outlines the goals, direction, concepts, and basic rules for managing information security.

**Focus Area:**

This Policy is relevant to the entire ISMS procedure.

**Usable Parties:**

This document can be used by all employees who are part of the ISMS scope and by relevant external parties.

# Reference Documents

* ISO 27001 Standards, clause 5.2
* List of legislation and contractual requirements document

# Terminology used in information Security

* **Confidentiality:** Only authorized parties should have access to the information.
* **Integrity:** The information shouldn't be changed by anyone who isn't authorized.
* **Availability:** Information is always accessible for those who have permission.

## Principle

Information security is managed based on risk, legal and regulatory requirements, along with business needs.

## Commitment from the top executives

Managing data is really important for our organization, and keeping that data safe is a top priority for our management team. We take our responsibilities seriously when it comes to employee and customer information, making sure to follow GDPR and the Data Protection Act 2018 closely.

[Officer Name - Chief Executive] [Date & Signature]

## Objectives of Information Security Policy

Our main objectives are to ensure that the company follows GDPR regulations closely, along with maintaining the confidentiality, integrity, and availability of all sensitive information. The goals focus on using effective risk management techniques, adhering to legal and regulatory requirements, fulfilling contractual commitments, and meeting business needs. We will commit the necessary resources to create, implement, and enhance our Information Security Management System (ISMS). A key objective is to effectively manage information security risks, particularly when collaborating with third-party providers that handle, store, and transport data. We also aim to foster a culture of data protection and information security across the firm by implementing comprehensive training and education programs.

## Framework of Information Security Policy

The ISMS is developed using the information security policy framework. According to this policy, the policies that comprise the policy framework are mentioned below.

* DP 01 Data protection policy
* DP 01 Data retention policy
* IS 01 Information Security policy
* IS 02 Access Control policy
* IS 03 Access Management policy
* IS 04 Risk Management policy
* IS 05 Information Classification and Handling policy
* IS 06 Information Security Awareness and Training policy
* IS 07 Acceptable Use Policy
* IS 08 Clear Desk and Clear Screen policy
* IS 09 Mobile and Teleworking policy
* IS 10 Business Continuality policy
* IS 11 Backup policy
* IS 12 Malware and Antivirus policy
* IS 13 Change Management policy
* IS 14 Third Party Supplier Security policy
* IS 15 Continual Improvement policy
* IS 16 Logging and Monitoring policy
* IS 17 Network Security Management policy
* IS 18 Information Transfer policy
* IS 19 Secure Development policy
* IS 20 Physical and Environment security policy
* IS 21 Cryptographic Key Management policy
* IS 22 Cryptographic control and encryption policy

# Information Security Roles and Responsibilities

Everyone has the responsibility to keep information secure, which means it's important to fully understand and follow the rules and practices that are in place. All suspected or confirmed violations should be reported right away.

* **Monitoring process:**
* The Review Management Unit is in charge of managing the ISMS.
* There are scheduled times for carrying out independent internal and external audits to evaluate the ISMS.
* **Legal and Regulatory Obligation**
  + The company really focuses on making sure it follows all the legal and regulatory rules it has to.
  + We keep detailed records of these requirements in the "Legal and Contractual Requirements Register."
* **Awareness and Training of Information Security Policy**
  + To make sure everyone, both inside and outside the organization, understands everything clearly, all policies are written in a straightforward way.
  + The paper on the "Competency Matrix" provides a clear definition and documentation of the training needs.

# Policy Compliance

* **Measurement**

The Information Security Management Unit will check how well policies are being followed by using different methods, like internal audits and providing feedback to the policy owner.

* **Exceptions**

The information security manager must authorize and accurately record any exceptions. These exceptions are promptly conveyed to the Management Review Team.

* **Non-Compliance**

Employees who contravene the policy may incur disciplinary measures, potentially resulting in termination of employment.

* **Continuous Improvement**

The policy is regularly updated as part of our commitment to ongoing improvement to ensure continued advancement.

# 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]

As the owner of this document, [job title] bears the responsibility of conducting periodic checks and making necessary updates, with a minimum frequency of once a year.

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

* All documents must be created in accordance with the procedures outlined in this document.
* Every document must undergo a controlled process for creation, approval, distribution, utilization, and updates.

[Job Title]

[Name]

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

[Signature]

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

[signature]