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

**Information Security Policy**

|  |  |
| --- | --- |
| 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](#_Toc84476003)

[2. Reference Documents 5](#_Toc84476004)

[3. Terminology used in information security 5](#_Toc84476005)

[3.1. Principle 6](#_Toc84476006)

[3.2. Commitment from the top executive 6](#_Toc84476007)

[3.3. Objectives of Information Security Policy 6](#_Toc84476008)

[3.4. Framework of Information Security Policy 7](#_Toc84476009)

[3.5. Information Security Roles and Responsibilities 8](#_Toc84476010)

[3.5.1. Monitoring process 8](#_Toc84476011)

[3.5.2. Obligations in Legislation and Regulatory 8](#_Toc84476012)

[3.5.3. Awareness and Training of the Information Security Policy 8](#_Toc84476013)

[4. Policy Compliance 9](#_Toc84476014)

[4.1. Measurement 9](#_Toc84476015)

[4.2. Exceptions 9](#_Toc84476016)

[4.3. Non-compliance 9](#_Toc84476017)

[4.4. Continual Improvement 9](#_Toc84476018)

[5. Maintaining control of records based on this document 10](#_Toc84476019)

[6. Validity and Document Management 10](#_Toc84476020)

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

Objective

This top-level Policy defines the goal, direction, principles, and core rules for information security management.

Focus Area

This Policy applies to whole ISMS procedure.

Usable parties

This document is accessible to all workers covered by the ISMS as well as any pertinent third parties.

# Reference Documents

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

# Terminology used in information security

Confidentiality

Information must only be available for authorized parties.

Integrity

The Information must not be modified by unauthorized parties.

Availability

Information always available for authorized parties.

## Principle

Information security is managed based on risk, statutory and regulatory requirements, and business needs.

## Commitment from the top executive

Information handling is crucial to our company's operations, and the management's top priority is to preserve and safeguard that data. We take our obligations under the GPDR and the Data Protection Act 2018 extremely seriously, whether it involves the data of our customers or our workers. [Officer name, data, and signature of Chief Executive]

## Objectives of Information Security Policy

* To uphold the company's confidentiality, integrity, and availability, as well as any private information, as outlined by the GPDR, in accordance with sound risk management, legal, contractual, and regulatory requirements, as well as business needs.
* To offer the resources required for designing, implementing, and improving the ISMS.
* To efficiently manage third-party suppliers who handle, store, or transport data in order to reduce and manage information security risks.
* To instill a culture of data security and protection through in-depth instruction and training.

## Framework of Information Security Policy

Based on the information security policy framework, the ISMS is created. The regulations that make up the policy structure are listed below in accordance with this policy.

* DP 01 Data protection policy
* DP 02 Data retention policy
* IS 01 Information Security policy
* IS02 Access Control policy
* IS 03 Asset 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 is accountable for information security, which includes being aware of and abiding by the rules, following instructions, and reporting any infractions.

### Monitoring process

The Examination Management Unit keeps an eye on the ISMS. Internal and exterior audits of the ISMS are conducted on a regular basis and independently.

### Obligations in Legislation and Regulatory

The organisation takes its legal and regulatory obligations seriously, and records of them are kept in a "Legal and Contractual Requirements Register."

### Awareness and Training of the Information Security Policy

In order for those inside as well as outside to grasp the policies, they should all be more verbose. The document "Competency Matrix" lists the training criteria that have been established.

# Policy Compliance

## Measurement

By using a variety of techniques, such as internal audits, feedback to the policy owner, and more, the leadership team of information security will assure compliance with this policy.

## Exceptions

Exceptions are authorized, filed, and sent to the management assessment team by the supervisor of information security..

## Non-compliance

Any employee who violates the policy may face disciplinary action, including termination of employment.

## Continual Improvement

The policy should update periodically to maintain the continual improvement.

# 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]

[job title] is the owner of this document who has the responsibility to check and if required update the record at least as per once a year.

[job title]

[name]

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

[signature]