**Information Security Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_gq9b4kgz8fcp) **2**

[**Table of Contents**](#_7okx9mf0bxe5) **3**

[**Purpose**](#_doug72wctets) **4**

[**Scope**](#_3dy6vkm) **4**

[**Policy**](#_1t3h5sf) **4**

[**Policy Communication Strategy**](#_4d34og8) **4**

[**Security Awareness training**](#_2s8eyo1) **5**

[**Change, Review, and Update**](#_w1o88vxspwq8) **5**

[**Disciplinary Action**](#_1b64a7ktf8py) **5**

[**Responsibility**](#_3z6f7qtfare9) **5**

[**Related Documents**](#_pgexw9pbtts8) **5**

## 

## ***Purpose***

The purpose of this policy is to ensure the organization has a set of information security policies designed to direct the behavior of individuals in a manner that is adequate and proportionate to associated risks.

## ***Scope***

This policy applies to all employees of *[Company]*. The policy relates to information managed or associated with *[Company]* that it is being stored or processed using *[Company]’s* facilities including its accommodation, equipment, computers, and networks, or privately-owned equipment.

The policy covers all information management and processing activities.

## ***Policy***

1. he organizational Information Security Policy is the top-level policy below which all other information security policies are subordinate.
2. All subordinate policies must adhere to and support the organizational Information Security Policy.
3. Each policy will have an owner who is responsible for:
   1. Ensuring the policy is understandable; pragmatic & enforceable; adequate & proportionate, and made available to relevant personnel (who may be external to the organization).
   2. Policy review and maintenance in line with:
      1. review of the policies for information security.
      2. logging and authorization of policy waivers and exceptions.
4. Policies must be approved by authorized management.
5. Policies will be made available to all relevant personnel.
6. Any policy made available must be read, understood and complied with.
7. Any waivers or exceptions to policies must be authorized by the relevant policy owner, logged and managed.

Subordinate policies include, but are not limited to:

* *[provide the list of all relevant security policies, that cover ISMS processes in the company]*.

## ***Policy Communication Strategy***

Information Security Policy and all its sub-policies are uploaded to the corporate Confluence which is accessible to all of *[Company]’s* employees. The procedures defined in those policies are all assigned to the responsible personnel. Employees involved in implementing the procedures are communicated about their direct responsibilities via email.

## ***Security Awareness training***

The company communicates information to improve security knowledge and awareness as well. That is why *[Company]* implemented an awareness training program to model the appropriate security behaviors of the employees. The awareness training includes the security awareness course with the test as a knowledge check. After finishing the course each employee gets a certificate about the successful completion of the course. Taking a security awareness course is necessary for every IT-related employee of *[Company]*.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Asset Management Policy
* Supply Chain and Business Partner Policy