|  |
| --- |
| information security policy  Free to use example |
| Let’s boost up your security  Version 1.0 Created by: securitybooster.net |



# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Rationale** |
| 0.1 | 01-06-2022 | J. Smith, security team | First draft |
| 1.0 | 15-06-2022 | J. Doe, board of directors | Approved version release |
| 1.1 | 04-11-2022 | F. Jacobs, security team | Updated responsibility chapter to better match the current the organization |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Purpose

For <name of the organization> it is important that the long term strategy and goals are realized in order to support its clients. As <name of the organization> is in possession of sensitive data, it is important to keep this data save. This document is intended for all employees and contractors of <name of organization> who have access to <name of the organization>’s data in any way.

# Definition of Information Security

Information security is a set of preventive, detective, repressive and corrective measures which guarantee the confidentiality, integrity and availability of data. Its purpose is to make sure the impact of an security incident is limited to an previous accepted level.

# Scope

This policy applies to all employees and contractors of <name of organization> and any others who may process information on behalf of <name of the organization>.

# Objectives

The objectives of this policy are:

* to avoid the disclosure of data
* to avoid causing financial and reputational damage
* to avoid breaking laws and regulations which are relevant for <name of the organization>
* to raise awareness

# Principles

The following principles are set to support this policy:

* Information will be made available solely to those who have legitimate need for access
* It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification
* Information will be protected against unauthorized access
* All information will be classified according to an appropriate level of security
* Compliance with the information security policy will be enforced

# Commitment

This policy has been approved by the Board of Directors of <name of organization> on <date> and will be reviewed annually by the Chief Information Officer. Any changes to this policy must be approved by the Board of Directors.

# Roles and Responsibilities

The following roles and responsibilities are most important for this policy:

Executive Management is responsible for the strategic approach to information security, agreeing on risk appetites and holding high level risks beyond this point.

The Chief Information Officer is responsible that the review of this policy takes place and to ensure that this policy remains internally consistent.

The Chief Information Security Officer is responsible for the implementation and maintenance of an effective Information Security Management System.

All employees of <name of the organization> must be aware of this policy and its content.

# Exceptions

As the information security policies are set to secure the information of <name of the organization>, occasionally exceptions on the policy will exist.. Any (temporary) exception on an information security policy must be reported to the Information Security Officer and include a risk analyses.

# Supported documents

The following documents are available for all employees on the intranet website and support this policy in more detail:

* Asset Management
* Business Continuity Management
* Classification policy
* Compliance
* Encryption
* Human Resources
* Information Access Management
* Mobile and Remote Working
* Monitoring and logging
* Physical Security
* Privacy and Personal Identifiable Information
* Secure Development
* Security Incident Handling
* Secure System Management
* Vendor Management