[Organization logo]

[Organization name]

INFORMATION SECURITY POLICY

Code:	
Version:	
Date of version:	
Created by: Approved by:	
Confidentiality level:	

Commented [27A1]: To learn how to fill out this document, and to see real-life examples of what you need to write, watch this video tutorial: "How to Write the ISMS Policy According to ISO 27001".

To access the tutorial: In your Inbox, find the email that you received at the moment of purchase. There, you will see a link and a password that will enable you to access the video tutorial.

Commented [27A2]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [27A3]: This article will help you understand the purpose of Information Security Policy:

Information security policy – how detailed should it be?
https://advisera.com/27001academy/blog/2010/05/26/information-security-policy-how-detailed-should-it-be/

Commented [27k4]: This article will help you understand the content of Information Security Policy:

What should you write in your Information Security Policy according to ISO 27001?
https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/

Commented [27A5]: If you need a document that will provide detailed rules for information security, then please use the IT Security Policy included in the toolkit.

You can separately purchase the IT Security Policy here:
https://advisera.com/27001academy/documentation/acceptable-use-policy/

Commented [27A6]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of [organization name], as well as relevant external parties.

2. Reference documents

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- ISMS Scope Document
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Legal, Regulatory and Contractual Obligations
- *
- [Business Continuity Policy]
- [Incident Management Procedure]

Commented [27A7]: List other internal documents of the organization associated with this Policy - for example, strategic development plan, business plan, document on strategic risk management, etc.

Commented [27A8]: See item 4.4

Commented [27A9]: See item 4.5

3. Basic information security terminology

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

[illegible]

Information security – preservation of confidentiality, integrity and availability of information.

[illegible]

4. Managing the information security

4.1. Objectives and measurement

[illegible]

Commented [27A10]: [illegible]

the organization's business objectives, strategy and business plans. [Job title] is responsible for reviewing these general ISMS objectives and setting new ones.

[redacted]

All the objectives must be reviewed at least once a year.

[Organization name] will measure the fulfillment of all the objectives. [Job title] is responsible for setting the methods for measuring the achievement of the objectives – the measurements will be [redacted] Measurement Report.

4.2. Information security requirements

This Policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organization in the field of information security, as well as with contractual obligations.

[redacted]

4.3. Information security controls

[redacted]

The selected controls and their implementation status are listed in the Statement of Applicability.

4.4. Business continuity

Business continuity management is prescribed in the Business Continuity Management Policy.

4.5. Responsibilities

Responsibilities for the ISMS are the following:

- [job title] is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- [redacted]
- [redacted]
- [job title] will implement information security training and awareness programs for employees

Commented [27k11]: To learn more about alignment between ISO 27001 and the business, please see this article:

Aligning information security with the strategic direction of a company according to ISO 27001
https://advisera.com/27001academy/blog/2017/02/20/strategic-direction-of-a-company-according-to-iso-27001/

Commented [27k12]: [redacted]

Commented [27A13]: Assess whether this frequency is appropriate.

Commented [27A14]: You'll find this template in the folder "Management Review".

Commented [27A15]: List also other fields which are regulated by the local legislation - e.g. data secrecy, business continuity, personal data protection, etc.

Commented [27A16]: Delete this section if business continuity will not be implemented.

Commented [27k17]: To get a better understanding of Top Management responsibilities, please see this article:

Roles and responsibilities of top management in ISO 27001 and ISO 22301
https://advisera.com/27001academy/blog/2014/06/09/roles-and-responsibilities-of-top-management-in-iso-27001-and-iso-22301/

Commented [27A18]: Member of top management.

Commented [27A19]: [redacted]

Commented [27A20]: [redacted]

- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- [illegible]
- [illegible]
- [job title] is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

4.6. Policy communication

[Job title] has to ensure that all employees of [organization name], as well as appropriate external parties are familiar with this Policy.

5. Support for ISMS implementation

Hereby the [job title or top management body in the scope of the ISMS] declares that ISMS [illegible] in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

6. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of employees and external parties who have a role in the ISMS, but are not familiar with this document
- non-compliance of the ISMS with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of ISMS implementation and maintenance
- unclear responsibilities for ISMS implementation

[job title]
[name]

_____
[signature]

Commented [27A21]: [illegible]

Commented [27A22]: [illegible]

Commented [27A23]: This training will help you train the employees, raise the security awareness and track their knowledge: https://training.advisera.com/awareness-session/security-awareness-training/

Commented [27k24]: [illegible]

Commented [27A25]: This is only a recommendation; adjust frequency as appropriate.

Commented [27A26]: The Policy must be approved by top management in the ISMS scope.

Commented [27A27]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.