[Organization logo]

[Organization name]

Commented [270012]: All fields in this document marked by square brackets [ ] must be filled in.

INFORMATION SECURITY POLICY

Commented [270013]: 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 [270014]: This article will help you understand the content of Information Security Policy:

What is the ISO 27001 Information Security Policy, and how can you write it yourself?
https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/

Commented [270015]: If you need a document that will provide detailed rules for information security, then use the IT Security Policy template included in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "09_ISO_27001_Annex_A_Security_Controls"

Commented [270016]: 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.

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

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.

Commented [270017]: Include the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses 5.2, 5.3, 6.2, 7.4, and A.6.3
- ISMS Scope Document
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Legal, Regulatory, Contractual and Other Requirements
- [Other internal documents]
- [Business Continuity Policy]
- [Incident Management Procedure]

Commented [27A8]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "04_ISMS_Scope".

Commented [27A9]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "06_Risk_Assessment_and_Risk_Treatment".

Commented [27A10]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "07_Applicability_of_Controls".

Commented [27A11]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "03_Identification_of_Requirements".

Commented [2700112]: List other internal documents of the

Commented [2700113]: See item 4.4

Commented [2700114]: See item 4.5

3. Basic information security terminology

or systems.

systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons

of planning, implementing, maintaining, reviewing, and improving the information security.

4. Managing the information security

better market image and reducing the damage caused by potential incidents; goals are in line with

Commented [2700115]: If necessary, change and/or add other

months."

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

[redacted]

Applicability.

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

[redacted]

responsible to record the details about measurement methods, periodicities and results in the Measurement Report.

[redacted]

A detailed list of all contractual and legal requirements is provided in the List of Legal, Regulatory and Contractual Obligations.

4.3. Information security controls

[redacted]

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

[redacted]

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]
- [redacted] employees

Commented [2700116]: To learn more about alignment between ISO 27001 and the business, 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 [2700117]: For information about the importance of control objectives, please see this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700118]: [redacted]

Commented [2700119]: Assess whether this frequency is appropriate.

Commented [2700120]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "13_Management_Review".

Commented [2700121]: [redacted]

Commented [2700122]: Delete this section if business continuity will not be implemented.

Commented [2700123]: To get a better understanding of Top Management responsibilities, 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 [2700124]: Member of top management.

Commented [2700125]: [redacted]

Commented [2700126]: [redacted]

Commented [27A27]: These are mandatory according to ISO 27001; do not delete them.

- the protection of integrity, availability, and confidentiality of assets is the responsibility of
- which applies to all persons who have a role in information security management

4.6. Policy communication

parties are familiar with this Policy.

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:

[job title]
[name]

[signature]

Commented [27A28]: Several responsible persons may be appointed, according to incident types.

Commented [2700129]: Or make a reference to the Incident Management Procedure.

Commented [2700130]: 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 [27A31]:

Commented [2700132]: Include the name of your organization.

Commented [2700133]: To get a better understanding of resource provision, please see this article:

How to demonstrate resource provision in ISO 27001 https://advisera.com/27001academy/blog/2017/04/10/how-to-demonstrate-resource-provision-in-iso-27001/

Commented [2700134]: This is only a recommendation; adjust frequency as appropriate.

Commented [2700135]: The Information Security Policy must be approved by top management in the ISMS scope.

Commented [2700136]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.