[Organization logo]

[Organization name]

Commented [20A1]: All fields in this document marked by square brackets [ ] must be filled in.

INFORMATION SECURITY POLICY

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

Commented [20A2]: 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	20000Academy	Basic document template

Table of contents

1. Purpose, scope and users

The aim of this document is to define the purpose, direction, principles and basic rules for information security.

This document is applied to all processes and activities of the SMS.

Users of this document are all employees of [organization name], as well as all external parties who have a role in the SMS.

Commented [20A3]: Please include the name of your company.

2. Reference documents

- ISO 20000-1:2018 clauses 8.7.3, 7.5.4.e)
- Information Security Management Process
- IT Service Continuity Management Process
- Service Availability Management Process
- Incident Management Process
- Change Management Process

Commented [20A4]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder "11_Service_Assurance_Processes/ 11.2_Service_Continuity_Management".

Commented [20A5]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder "11_Service_Assurance_Processes/ 11.1_Service_Availability_Management".

Commented [20A6]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder "10_Resolution_Fulfilment_Processes/ 10.1_Incident_Management".

Commented [20A7]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder "09_Service_Design_Build_Transition_Processes/ 09.1_Change_Management".

3. Definitions

[illegible] – 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] – characteristic of the information by which it can be accessed by authorized persons when it is needed.

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

[illegible] – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

4. Objective

The objective of Information Security Management is to provide confidentiality, integrity and [illegible].

The Information Security Manager is responsible to review goals for Information Security Management and set new ones [annually].

Commented [20A8]: You can adapt the frequency according to your company practices.

4.1. Information Security Policy

Information Security Policy is a guideline which provides rules for use and misuse of [organization name]'s information security.

[illegible]

[illegible]

- [illegible]

4.2. Information security requirements

Legal and regulatory requirements and contractual obligations relevant to the organization in the field of information security with which information security activities comply are listed in the SMS Plan.

[illegible]

4.3. Risk Management

[illegible] Risks and Opportunities Register. Risk level is calculated according to the agreed methodology. [illegible] [once a year].

4.4. Information security controls

[illegible]

- [illegible]
- [illegible]
- [illegible]

Effectiveness of controls is reviewed during the internal security audit. The Internal Audit Report contains necessary actions.

[Job title] is responsible to:

- [illegible]
- [illegible]

[illegible]

[illegible]

Commented [20A9]: [illegible]

Commented [20A10]: [illegible]

Commented [20A11]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “04_SMS_Plan”.

Commented [20A12]: [illegible]

Commented [20A13]: [illegible]

Commented [20A14]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “05_Risk_Management”.

Commented [20A15]: Change as needed. It could be, e.g. after a major incident.

Commented [20A16]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “12_Internal_Audit”.

Commented [20A17]: Please insert the appropriate job title according to your organization practices, e.g.: Information Security Manager, Supplier Manager and Service Level Manager.

Commented [20A18]: These are mandatory but you may include additional elements according to your company practices.

Commented [20A19]: [illegible]

Commented [20A20]: [illegible]

The Internal Auditor ensures that results of the audit are saved in the Internal Audit Report. The Continual Service Improvement Manager reviews audit results and defines opportunities for [illegible]

[illegible]

4.6. Policy communication

The Information Security Manager has to ensure that all employees of [organization name], as well as appropriate external parties [illegible] are familiar with this policy and the importance of conforming to the policy.

After each major change in the policy, [illegible] suppliers containing the new version of the document and a reminder regarding the importance of conforming to the policy.

4.7. Security incident management

Security incidents are managed by the Incident Management process. Information security incidents are classified as [...]. [illegible] incidents and comm[illegible]

[illegible]

Information security incidents are reviewed, and improvements are identified by the Information Security Manager.

5. Validity and document management

This document is valid as of [date].

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

[Job title] approves this policy.

[Job title]
[Name]

Commented [20A21]: [illegible]

Commented [20A22]: You can adjust this according to your company practices.

Commented [20A23]: You can adapt the frequency according to your company policies.

Commented [20A24]: [illegible]

Commented [20A25]: [illegible]

Commented [20A26]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Security Manager etc.

Commented [20A27]: This is only a recommendation; adjust frequency according to your company practices.

Commented [20A28]: Please insert the appropriate job title from the top management according to your organization practices, e.g.: CEO, CIO, IT Director, IT Manager, etc.

[organization name]

[Signature]

Commented [20A29]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.